S. Hrg. 108–683

AN ASSESSMENT OF CURRENT EFFORTS TO COMBAT TERRORISM FINANCING

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JUNE 15, 2004

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

95–189 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska	JOSEPH I. LIEBERMAN, Connecticut
GEORGE V. VOINOVICH, Ohio	CARL LEVIN, Michigan
NORM COLEMAN, Minnesota	DANIEL K. AKAKA, Hawaii
ARLEN SPECTER, Pennsylvania	RICHARD J. DURBIN, Illinois
ROBERT F. BENNETT, Utah	THOMAS R. CARPER, Delaware
PETER G. FITZGERALD, Illinois	MARK DAYTON, Minnesota
JOHN E. SUNUNU, New Hampshire	FRANK LAUTENBERG, New Jersey
RICHARD C. SHELBY, Alabama	MARK PRYOR, Arkansas

MICHAEL D. BOPP, *Staff Director and Chief Counsel*
DAVID A. KASS, *Chief Investigative Counsel*
EDWARD W. PRIESTOP, *Federal Bureau of Investigations Detailee*
JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*
DAVID BARTON, *Minority Professional Staff Member*
AMY B. NEWHOUSE, *Chief Clerk*

CONTENTS

WITNESSES

TUESDAY, JUNE 15, 2004

ALPHABETICAL LIST OF WITNESSES

APPENDIX

AN ASSESSMENT OF CURRENT EFFORTS TO COMBAT TERRORISM FINANCING

TUESDAY, JUNE 15, 2004

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:30 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Coleman, Specter, Lieberman, Levin, Akaka, Lautenberg, and Pryor.

OPENING STATEMENT BY CHAIRMAN COLLINS

Chairman COLLINS. The committee will come to order.

Good morning. Today the Governmental Affairs Committee will conduct a review of current efforts underway to combat terrorism financing.

This is the third hearing the Committee has held during the past year on this issue of great global importance. The focus of our hearing today is a new report by the Independent Task Force on Terrorism Financing sponsored by the Council on Foreign Relations. The Council's first report, released in October 2002, begins with these words: "The fog of war has long befuddled military and political leaders. Of all the battle fronts in today's war on terrorism, few are as foggy as efforts to combat terrorist financing."

As both of these reports make clear, however, this fog is no natural phenomenon. It is entirely manmade. Terrorism thrives in the shadows. It prospers by deceit and deliberate confusion. It is a perverted world in which murderers are called freedom fighters and in which building schools and health clinics can excuse the slaughter of innocents.

The answer is relentless scrutiny and then taking forceful and effective action.

This new report focuses primarily upon the actions taken by the Governments of the United States and of the Kingdom of Saudi Arabia. It provides an insightful analysis of the progress that has been made and of the challenges that remain.

As the report observes, Saudi Arabia has, on a comparative basis, taken more legal and regulatory actions to combat terrorism financing than many other Muslim States. However, the size, the reach and the wealth of persons and institutions there with connections to violent terrorist groups put the kingdom on the front lines of this battle.

There are other engines of terrorism financing, but as David Aufhauser, one of our distinguished witnesses, testified just 1 year ago, Saudi Arabia is, in many ways, the epicenter of terrorism financing. As the Council's first report stated, individuals and charities based in Saudi Arabia have been the most important source of funds for al Qaeda.

A phrase that occurs again and again throughout this new report is political will. In some instances, it is evident and growing. In others it is still woefully lacking. This mixed result characterizes Saudi Arabia. The Saudi government deserves credit for undertaking considerable legislative and regulatory reforms. Questions remain, however, about whether these reforms are being consistently, effectively, and vigorously implemented.

For example, the kingdom recently dissolved the notorious Al Haramain charity and it has created a new organization to coordinate and oversee private Saudi charitable giving abroad. This is a very positive step that should significantly diminish the ability of al Qaeda and other terrorist groups to raise and move funds using charities as conduits. There remain, however, serious questions. Most important, what are the Saudi's doing to crack down on the International Islamic Relief Organization, the World Assembly of Muslim Youth, and the Muslim World League, three of the charities alleged to have the most troubling terrorism connections.

Terrorists attacking Saudi Arabia from within the country have been killed and many Saudi law enforcement personnel have given their lives. Yet this report also notes that since September 11, 2001 we know of not a single Saudi donor of funds to terrorist groups who has been publicly punished.

Perhaps most troubling is the continued gap between what Saudi leaders say to the world and what some of them have to say to their own people. Following the al Qaeda attacks in early May, Crown Prince Abdullah said on Saudi TV that "Zionism is behind the terrorist attacks in the kingdom. . . . I am 95 percent sure of that." That astonishing and inflammatory remark was reiterated a few days later by the Saudi Foreign Minister. The Saudi Interior Minister then left no doubt as to the meaning when he bluntly stated that al Qaeda is backed by Israel.

This is not just a lack of political will. This is political blindness. To say that the Kingdom of Saudi Arabia is a full partner in the war against terrorism while such inflammatory and anti-Semitic statements are being made would certainly be vastly premature.

On an encouraging note, the report details significant progress by the U.S. Government in combating terrorism financing. A key recommendation of the first task force report in 2002 was for the Administration to centralize the coordination of efforts to combat terrorism financing. This has been accomplished to a significant degree.

The Administration also deserves credit for prompting the Saudis to begin to undertake serious reforms and to extend meaningful cooperation to American terrorism investigations. The progress represented by the enactment of the Saudi legal reforms, the Saudi actions against al Qaeda cells in the kingdom, and the creation of the Joint Terrorism Financing Task Force should not be understated. These are indeed important achievements.

But the report also finds several troubling shortcomings and includes a number of thought-provoking recommendations for change. I am particularly intrigued by the task force's recommendation for Congress to enact a certification regime that would require the President to certify whether foreign nations are fully cooperating with the fight against terrorism financing. If the President did not make this certification or issue a waiver in the interest of national security, non-cooperating nations would face an array of sanctions. This type of regime has been employed in the war on illegal drugs. The report suggests that it be in place for the fight against terrorist funds as well.

We, the Governments of the United States, Saudi Arabia, and all responsible nations, have made considerable progress in combating terrorism. But this struggle is not easily won and money remains the lifeblood of many terrorist operations. We must not rest until we have done everything in our power to halt the flow of money that breathes life into these groups. We must exercise relentless scrutiny and take strong action. And as this report emphasizes so clearly, we must have the sustained will necessary to win the war against terrorism.

Senator Lieberman.

OPENING STATEMENT BY SENATOR LIEBERMAN

Senator LIEBERMAN. Thank you very much, Chairman Collins for convening this hearing, and also, I must say, for that excellent opening statement.

Our subject for today is about one of the most important battlefronts in our war against terror and that is the effort to stop the funding of terrorists. If we can succeed in choking off the money that sustains terrorist activities we can literally reduce the death and destruction the terrorists cause.

The Council on Foreign Relations, in its report today, has done a real service. The report should help us refocus, reexamine and redouble our efforts to cut off the flow of money to international terrorist groups. Of course, that includes leading us to take again a hard and demanding look at financial support for terrorism from Saudi Arabian sources.

Immediately after September 11, President Bush signed an executive order aimed at blocking terrorist funds. In one sense our overarching question in this hearing and our Committee's continuing investigations is what progress has been made in implementing that order.

It is clear that in the first few months following the President's announcement there was very significant success. Over $100 million in terrorist money was blocked or frozen around the world. But, in the 2 years since then only $30 million has been stopped. So that both the United Nations Monitoring Group on Terrorist Financing and Congress's own General Accounting Office concluded at the end of 2003 that American efforts have sadly not stemmed the flow of money to terror groups.

We will want to ask our witnesses today why this has happened and what we can do together to make sure that we do cut off the flow of money. The Council on Foreign Relations report does sug-

gest the beginning of a series of answers about where some of the problems may be.

I thought one surprising possible cause that the report cites is the fact that the Administration has only used new authorities under the Patriot Act, the much-maligned Patriot Act, to crack down on the assistance of foreign financial institutions for terrorism only one time and that was quite recently against a Syrian bank. I would like to get a little background about why we think that has happened and whether the witnesses believe that there are other areas in which we can use that Patriot Act authority.

Second, the Council report tells us that the coordination of America's efforts to block terrorist funding has bounced around a bit among the National Security Council, the Counsel of the Treasury Department, and the FBI. In fact, there have been five different people in charge since September 11. And, that uncertainty and changes in leadership may have undermined the coordination and the effectiveness of our anti-terror financing efforts.

Leadership has now shifted, with some clarity it appears to me, to the National Security Council, although not through any formal process that would give it continuity and institutional permanence. I think that is greatly to be desired.

I note for the record the nodding of at least two of the witnesses to that suggestion.

I do also note that one of our witnesses today, former Treasury Department General Counsel David Aufhauser, believes that this leadership role, in fact, should reside at the Treasury Department. I would be interested in hearing his views on that matter during his testimony.

But either way, whether at the Treasury Department or at the NSC, leadership has got to be made certain, and in that sense, institutionalized. It should no longer be left to ad hoc and uncertain arrangements.

The Intelligence Committees of Congress reported a while back in their joint inquiry into September 11 that the tendrils of Bin Laden's al Qaeda terrorist network extend into as many as 60 countries. That means our war against this network and those who finance it must be just as extensive.

The Council reports, hopefully, that 117 nations have signed now the International Convention to Suppress Terror Financing, which is up from four at the time of the September 11 attacks. So we have gone from four countries who are signatories to 117. That is the good news.

The bad news is that most of those countries, the Council reports, do not have either the actual tracking capabilities or the resources to track laundered money. I want to hear from the witnesses about what we can do to make that bad news better.

In working to cut off funding for terrorism, Saudi Arabia, long a very important and close ally of the United States of America, becomes a necessary focus of attention. Bin Laden was a Saudi but more to the point 15 of the 19 September 11 hijackers were Saudis and questions continue to remain about financial connections between Saudi money and terror funding within the United States.

Before the May 2003 terrorist bombings in Riyadh many independent analysts, including the Council on Foreign Relations, have

told us that Saudi officials may have talked the talk on cooperating with the United States in the blocking of terrorism financing and investigating and prosecuting of those who were involved in it. But then, in many cases, did not walk the walk. In fact, they turned a blind eye to Saudi money going to organizations directly or indirectly supporting terrorism.

Again, I stress that is not my conclusion, that is the conclusion of many independent analysts. Today's CFR report points encouragingly to positive signs of intelligence sharing and law enforcement cooperation between the Saudis and the United States, again particularly since the May 2003 bombings in Riyadh. It says there is evidence that the actions taken by the Saudi government since then have actually hindered Bin Laden's financial operations and forced foreign-based terror groups to begin to try to raise their funds locally. That cooperation and progress between the United States and the Saudis is important and must grow.

In fact a joint U.S.-Saudi task force on these subjects was established last August to help the Saudis clamp down on terrorism financing, but the Council report tells us jarringly that the work of the joint task force has not led yet to one public arrest or prosecution of anyone in Saudi Arabia for financing terrorism. And that is hard to understand, particularly as the Council on Foreign Relations report indicates that there are two Saudis named Yasin Qadi and Wa'el Hamza Julaidan, who have been declared financiers of terrorism by the U.S. Government.

So we have made some progress in tracking and stopping terrorist financing but we, in Congress, still need to consider whether our urgent need to starve the terrorists of funding is being hampered by an uncertain organizational structure, by turf battles and perhaps by continuing defensiveness about our special relationship with the Saudi government and the Saudi ruling family.

In a day and age of terrorism which brings death and destruction not just to us and others but to Saudis themselves, we ought to be able best to preserve our relationship with the Saudis with total honesty and the most aggressive joint efforts against terrorism.

The CFR report and today's hearing, I hope, will begin to give us some answers to these questions which have become, in fact, life and death questions.

Thank you, Chairman Collins.

Chairman COLLINS. Thank you Senator. Senator Coleman.

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. Thank you, Chairman Collins. And thank you for your commitment to relentless scrutiny of this issue by holding a series of hearings on the report by the Council on Foreign Relations regarding terrorist financing.

Just two observations. One, it is clear that a new framework for the U.S.-Saudi relationship needs to be put into play focusing on accountability, accountability for terrorist financing. We have to see concrete results.

Second, in light of last week where we had a celebration of the life of Ronald Reagan and his optimism and belief that we would win the Cold War, and we did, I have the same optimism that we are going to win this struggle against terrorism, the same opti-

mism. But it is going to take resolve, it is going to take commitment. This report and these series of hearings go a long way to bolstering that optimism and making it a reality.

So again, I look forward to hearing the witnesses' testimony. Thank you for your leadership.

Chairman COLLINS. Senator Lautenberg.

OPENING STATEMENT OF SENATOR LAUTENBERG

Senator LAUTENBERG. Thank you, Madam Chairman, for holding this important hearing.

President Bush has said it, that money is the lifeblood of terrorism. And if we want to win the global war on terrorism, it is critical that we find out who is financing terrorism, how they are doing it, what we can do to stop it. And I am disappointed that we do not have any Administration official available to us today but these are good witnesses, Madam Chairman, and I am sure we will learn a lot.

Cooperation between Congress and the Administration is imperative. And we face a daunting challenge when it comes to attacking the financial infrastructure that makes terrorism function. That is why I am puzzled that we did not take an obvious step a few weeks ago when I offered an amendment to the Department of Defense Authorization Bill to close the loophole that allows American companies to do business through foreign subsidiaries with nations that sponsor terrorism.

I salute Chairman Collins for her vote. The amendment was defeated 49 to 50 and I am grateful that the Chairman was one of three Republicans to support the amendment. And I hope that she has the capacity to convince the rest of the caucus of the amendment's merits because I will keep offering it until the Senate adopts it.

For the life of me, I do not know how we can condone U.S. companies doing business with rogue states like Iran. 60 Minutes had a segment just a few months ago detailing an interest that, for instance, Halliburton had with a sham foreign subsidiary in the Grand Caymans so that it could sell oil field equipment to Iran. Nothing more, by the way, than an address, a drop station. There was nothing else there. But it enabled Halliburton to do business with Iran and other rogue states.

I have had members of my staff look into this and sure enough they found evidence of the business activity that existed between this subsidiary and a London-based subsidiary of the National Iranian Oil Company called Kala Limited. The State Department has verified that Iran supports Hamas and Hezbollah and Islamic Jihad.

I was in Israel some years ago when a terrorist attack by Islamic Jihad killed eight people. And I was there just a few weeks ago when a terrorist killed 10 people in the port city of Ashtarak. And we cannot forget when Hezbollah attacked the Marine barracks in Beirut, killing 241 of our soldiers.

Does it make sense for an American company to help Iranians produce oil more efficiently when they use those extra profits to finance terrorist groups that have killed Americans? I went to four viewings and funerals last week in the State of New Jersey, people

who died in the service of their country. And to think that an American company could be helping to finance indirectly those terrorist organizations is a national disgrace. We had a chance to close that loophole and we failed.

I am also concerned, as was suggested by Chairman Collins and by the Ranking Member, Senator Lieberman, about the complicity that seems to be in existence in Saudi Arabia and without criticism coming sufficiently from the Administration. Saudi Arabia still has not designated groups like Hamas as terrorist organizations. And as much as 60 percent of Hamas' annual budget is donated from Saudi sources. And although the Saudis have passed some anti-money-laundering laws, they do not seem to be enforcing them.

So I appreciate that we have a delicate relationship with countries like Saudi Arabia. But if we are going to protect Americans, which is the primary concern, here and abroad from the scourge of terrorism, we have got to find out who is financing it even if we disturb some of our buddies in the process.

I thank you, Madam Chairman, for holding this hearing.

Chairman COLLINS. Senator Pryor.

Senator PRYOR. I do not have any opening statement. Thank you.

Chairman COLLINS. Thank you, Senator. Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Madam Chairman.

I want to commend you for having this hearing and we hope that it will strengthen our capability to address the threats and challenges of terrorism financing.

I have a statement that I would like to place in the record. I just want to thank you again for holding this hearing and I look forward to hearing our witnesses and working with my colleagues on this important problem. Thank you.

[The prepared statement of Senator Akaka follows:]

PREPARED OPENING STATEMENT OF SENATOR AKAKA

Madam Chairman, thank you for holding this hearing. I hope it will help to strengthen our capability to address the threats and challenges of terrorism financing.

Last July, Mr. Pistole, from the Federal Bureau of Investigation reminded this Committee that identifying and dismantling the financial structures of terrorist groups is critical to preventing future attacks. We must heed Mr. Pistole's words especially as terrorist attacks continue to rise.

It is disheartening that almost three years after September 11, terrorist groups, including al Qaeda, continue to maintain sophisticated financial networks. What is more alarming is that sources attribute at least 60 percent of Hamas and al Qaeda funds to Saudi-based entities. Most of these funds are diverted from charities and businessmen to terrorist groups and are used to execute attacks or to entice new recruits.

Earlier this month, Saudi Arabia pledged it would dissolve the Al-Haramain Islamic Foundation, which U.S. officials allege to be al Qaeda's largest financial supporter, contributing $50 million on an annual basis. The National Commission for Relief and Charity Work Abroad will merge the assets of Al-Haramain and other Saudi-based charities into one account and ensure their legitimate use. But, Saudi officials have not yet specified whether the Commission will oversee charities with known terrorist connections.

I am concerned that this may be another promise that the Saudis cannot fulfill.

Last May, the Saudi government announced it would establish the High Commission for Charities to address Saudi-based groups financing terrorism. As of February of this year, no proposed budget or staff existed for this Commission. Furthermore,

no action has been taken against Al-Haramain's former leader, Al-Aqil, despite Saudi Arabia's promises to conduct criminal proceedings.

In addition, Saudi officials have not provided sufficient support to the Saudi Arabian Monetary Agency nor has the Saudi government created a financial intelligence unit.

Today, many view the U.S. and Saudi Joint Task Force on Terrorism Financing as a test of Saudi Arabia's responsiveness to terrorism. This collaboration will be an opportunity to gauge the Saudi's willingness to block the flow of money from its general and elite populations to terrorist organizations. I hope this task force will mark the beginning of progress.

I look forward to hearing from our witnesses and to working with my colleagues to address this critical issue.

Thank you.

Chairman COLLINS. Thank you, Senator. Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Madam Chairman, thank you, and thank you for your continuing leadership in this effort.

Since the September 11 attacks, this Committee has focused needed attention on the role of Saudi Arabia and the Saudia-based charitable organizations and terrorist financing. Today's hearing is the third in a series focusing on this issue over the past year. And I commend you again, Madam Chairman, for sustaining this Committee's strong oversight tradition for this critical issue.

Today's hearing focuses on a report authorized by the nonpartisan Council on Foreign Relations. It builds on a prior Council report issued nearly 2 years ago. It offers a number of important and practical suggestions including revitalizing the international effort led by the Financial Action Task Force to convince jurisdictions to strengthen their anti-money laundering efforts and improving the U.S. Government's sharing of terrorist financing information with U.S. financial institutions so that they can do a better job.

I want to focus just for a moment on one of the primary topics examined in the report and that is the role of Saudi Arabia. Right now, Saudi Arabia has two primary exports to the rest of the world: Oil and an extreme form of Islam that advocates hatred and violence to achieve its ends. Two exports, both having a huge impact on the world.

The report before us today does not shy away from the reality of that second export. It describes the "fundamental centrality that persons and institutions based in Saudi Arabia have had in financing militant Islamic groups on a global basis."

And then it repeats a statement that was made in its earlier report which is worth repeating, and that is that "it is worth stating clearly and unambiguously what official U.S. Government spokespersons have not. For years individuals and charities based in Saudi Arabia have been the most important source of funds for al-Qaeda; and for years Saudi officials have turned a blind eye to that problem."

Madam Chairman, because of the number of witnesses that we have I would ask that the balance of my statement be placed in the record at this time.

[The prepared statement of Senator Levin follows:]

PREPARED OPENING STATEMENT OF SENATOR LEVIN

Terrorists need money to carry out acts of terrorism. They need money for explosives, for communications, for travel, and for all the other details involved in carrying out plans for mass murder and mayhem. Global terrorist organizations need global financing. They need to be able to transfer funds across international lines, move money quickly, and minimize inquiries into their finances, their activities, and their supporters.

Since the September 11 attack, stopping terrorist financing has become a U.S. priority. This Committee has contributed in a significant way to that priority. First, prior to the attack, the Committee's Permanent Subcommittee on Investigations conducted a 3-year anti-money laundering investigation which produced extensive hearings and reports, documented little known methods for transferring illegal funds into the United States, and identified ways to strengthen U.S. laws to stop money laundering and terrorist financing. In early 2001, I introduced a bipartisan bill, S. 1371, with specific legislative proposals for strengthening U.S. anti-money laundering laws. The Senate Banking Committee utilized them in Title III of the USA Patriot Act, which was enacted into law in October 2001, 6 weeks after the September 11 attack.

Additionally, since the attack, this Committee has focused needed attention on the role of Saudi Arabia and Saudi-based charitable organizations in terrorist financing. Today's hearing is the third in a series focusing on this issue over the past year, and I commend Chairman Collins for sustaining the Committee's strong oversight of this critical issue. In the last Committee hearing on this topic, a key government official stated that "in many ways, [Saudi Arabia] is the epicenter" for financing of al Qaeda and other terrorist movements. Today's hearing focuses on a report that carries much the same message.

This report is authored by the nonpartisan Council on Foreign Relations. It builds on a prior Council report issued nearly 2 years ago, and addresses both the global campaign against terrorist financing and the additional steps that need to be taken by the United States and Saudi Arabia to combat terrorist financing. It offers a number of important and practical suggestions, including revitalizing the international effort led by the Financial Action Task Force to convince jurisdictions to strengthen their anti-money laundering efforts and improving the U.S. Government's sharing of terrorist financing information with U.S. financial institutions so they can do a better job.

I want to focus for a moment on one of the primary topics examined in the report and that is the role of Saudi Arabia. Right now, Saudi Arabia has two primary exports to the rest of the world: Oil and an extreme form of Islam that advocates hatred and violence to achieve its end.

The report before us today does not shy away from this reality. It describes "the fundamental centrality persons and institutions based in Saudi Arabia have had in financing militant Islamist groups on a global basis." It repeats a statement made in its earlier report:

> "It is worth stating clearly and unambiguously what official U.S. Government spokespersons have not: For years, individuals and charities based in Saudi Arabia have been the most important source of funds for al-Qaeda; and for years, Saudi officials have turned a blind eye to this problem."

The report cites with approval Saudi actions over the past 2 years to overhaul its anti-money laundering laws, increase its oversight of Saudi charities, and disrupt al Qaeda cells within the country. But it also faults Saudi Arabia for failing to prosecute a single individual involved with terrorist financing and for continuing to export radical extremism even while curbing it domestically.

For too long, Saudi Arabia has made a Faustian deal with the extremists who preach hatred and violence to achieve their ends, hoping that the violence these extremists advocate would not bloody the sands of Saudi Arabia itself. But recent events indicate that Saudi Arabia is beginning to reap what it has helped to sow worldwide, and that no one is safe from those who advocate terrorism to achieve their aims. The list of tragic events in Saudi Arabia resembles those in other countries ravaged by terrorism, with repeated bombings, kidnappings, and senseless death and destruction. On May 12 and November 9 of last year, for example, al Qaeda operatives bombed housing complexes used by foreign workers living in Riyadh, leading to the deaths of more than 50 individuals. This year saw an attack on Riyadh's General Security building followed by two attacks on Saudi oil facilities with the latter resulting in 22 fatalities. Now rumors allege a plot to kill Crown Prince Abdullah.

The report before us today advocates building a new framework for U.S.-Saudi relations that will include a frank acknowledgment of terrorist financing issues and the need to end Saudi support for radical extremism that condones violence. The plain fact is that, to stop terrorism, Saudi Arabia needs to stop financing radical clerics and madrassas that preach violence and hatred. It needs to publicly prosecute those who foment and finance terror. Ultimately, the Saudi government needs to recognize that it is not sufficient to selectively oppose terrorist groups that pose an immediate threat. The presence of any terrorist organization, regardless of its immediate focus, is a threat to all nations. For that reason, Saudi Arabia as well as our European allies need to cease funding for all terrorist groups, including Hamas and the charities that support it.

Of course, it is not just Saudi Arabia that needs to do more to fight terrorist financing. There is plenty that we in the United States need to do here at home. The report's recommendation that the U.S. conduct an analysis of Federal agencies to determine "who is doing what, how well and with what resources," is another way of saying that our current anti-money laundering and terrorist financing efforts are scattered, duplicative, and inefficient. There is no one top official in charge, little coordination, and less accountability.

The unfolding scandal at Riggs National Bank is another measure of our own weak anti-money laundering enforcement. Bank regulators recently imposed a $25 million fine on Riggs for its inadequate anti-money laundering efforts, but at the same time apologized for their own lax oversight in allowing Riggs to continue its failed policies and procedures for more than five years. Riggs has managed bank accounts not just for Saudi officials, but also for more than 100 other governments around the world. Recently, Riggs announced its intention to close many Embassy-related accounts due to high money laundering risks and the bank's inability to monitor them. These Embassies are now looking to open accounts at other banks. Federal regulators recently held a meeting with major U.S. banks to explain their expectations for managing these Embassy accounts. While the regulators insist this meeting was intended to spread the word about the need for due diligence, the media reported that others apparently interpreted the meeting as signaling regulatory support for taking on these accounts.

These mixed signals are a huge mistake. One of the lessons of the Riggs scandal must be that Embassy bank accounts can no longer operate with minimal scrutiny. Our banks and bank regulators must establish new rules and expectations. Embassy officials need to realize they can no longer engage in substantial cash transactions with no questions asked. Multiple Embassy accounts can no longer be opened with little or no due diligence. Suspicious transactions must be explained and justified. It can't be business as usual. Our security and the world's security depends upon it.

The 2002 report by the Council on Foreign Relations made a positive contribution to the fight against terrorist financing by saying a number of things that needed to be said openly and clearly and by making reasonable and practical suggestions. This second report has the potential to do the same. I thank today's witnesses for their service to our nation in contributing to this report and look forward to hearing their testimony today.

Chairman COLLINS. Thank you, Senator Levin.

I am delighted to welcome our witnesses this morning. We are extremely fortunate to have three such qualified experts to testify before us.

Lee Wolosky previously worked as the Director of Transnational Threats at the National Security Council. He is currently Counsel at the law firm of Boies, Schiller and Flexner and is an Adjunct Professor of International Affairs at Columbia University. Mr. Wolosky is also the Co-Director of the Independent Task Force on Terrorist Financing sponsored by the Council on Foreign Relations.

Mallory Factor is the President of Mallory Factor Inc., an independent merchant bank and financial relations firm that he founded in 1976. Mr. Factor has also worked as a Professor at the School of Continuing and Professional Studies at New York University and he serves as Vice-Chairman of the Task Force on Terrorist Financing.

We are also pleased to have with us for a second time David Aufhauser, who is now a member of the law firm of Williams and Connolly. He previously served as General Counsel of the Treasury Department from March 2001 to November 2003. At the Treasury Department, in addition to his responsibilities as General Counsel, Mr. Aufhauser served as the Chairman of the National Security Council's Policy Coordinating Committee on Terrorist Financing.

Thank you all for being with us today. We look forward to hearing your testimony. We will begin with you, Mr. Wolosky.

TESTIMONY OF LEE S. WOLOSKY,[1] CO-DIRECTOR, INDEPENDENT TASK FORCE ON TERRORISM FINANCING, COUNSEL, BOIES, SCHILLER AND FLEXNER, LLP

Mr. WOLOSKY. Thank you very much. Madam Chairman, Senator Lieberman and distinguished Members of the Committee, thank you for your kind words about our report and for your continuing leadership on terrorist financing issues.

This Committee's sustained attention to these issues is critically important to our Nation.

We are honored to report to you today on the Second Report of the Independent Task Force on Terrorist Financing sponsored by the Council on Foreign Relations. I have served as co-director of this bipartisan initiative since its founding in the Summer of 2002.

Our report is the result of the hard work of a number of dedicated individuals of both political parties to seek to further vital national interests. I wish to thank our Chairman, Maurice Greenberg, for his unwavering support of the task force. I would also like to thank our Vice-Chairman, Mallory Factor, and our Co-director and Co-author, William F. Wechsler, for all they have done to make the task force a success.

Finally, I am also grateful to Council President, Richard Haas, for his support and assistance to our work and it is an honor, let me add, to testify beside David Aufhauser, who served our country with dedication and distinction. Many of the positive developments in this area since September 11 are the direct fruits of his vision and leadership.

I will discuss the background of our second report and its findings. Mallory Factor will then discuss the report's recommendations.

Since the report, along with its various appendices, is almost 200 pages in length we will only be able to highlight core points and findings. We will ask that the full report and its appendices be entered into the record and we will look forward to a fuller discussion of various aspects of the report in response to your questions.[2]

In our first report, released in October 2002, we concluded "It is worth stating clearly and unambiguously what official U.S. Government spokespersons have not, for years individuals and organizations based in Saudi Arabia have been the most important source of funds for al-Qaeda and for years Saudi officials have turned a blind eye to this problem."

---

[1] The prepared statement of Mr. Wolosky appears in the Appendix on page 36.

[2] The report entitled "An Update on the Global Campaign Against Terrorist Financing," appears in the Appendix on page 54.

We recommended the encouragement of the Saudi regime to strengthen significantly its efforts to combat terrorist financing. In this regard, we noted a recent historical record of inattention, denial, and half measures.

We urged the U.S. Government to confront directly the lack of political will in Saudi Arabia and elsewhere through the institution of a declaratory policy that would permit or compel U.S. officials to speak more frankly about the nature of the problem.

The reaction to the release of the task force's initial report was reflective of then-prevailing mindsets. The Saudi Arabian Foreign Minister, for example, told *CNN* that the report was "long on accusation and short on documented proof."

The U.S. Treasury Department spokesperson called the report "seriously flawed."

The status quo changed on May 12, 2003 when al Qaeda bombed housing compounds in Riyadh used by Americans and other foreign residents, prompting more comprehensive Saudi action against terrorism. Public statements and actions by both the United States and Saudi Arabia since May 2003 have evidenced in many respects a more urgent approach to terrorist financing.

For example, Saudi Arabia has announced a profusion of new laws, regulations and institutions regarding money-laundering, charitable oversight and the supervision of the formal and informal financial services sector. Critically, for the first time, the Saudi Arabian government decided to use force to hunt and kill members of domestic al Qaeda cells, including, in one case, a financier known by the name of Swift Sword.

Saudi Arabia has markedly improved its tactical law enforcement and intelligence cooperation with the United States. The Bush Administration acted quickly to take advantage of the newfound political will in Saudi Arabia to renew and reinvigorate U.S. efforts to combat terrorist financing.

The Bush Administration also moved toward a more declaratory policy. On June 26, 2003, for example, David Aufhauser testified before the Congress that in many respects Saudi Arabia was an "epicenter" of terrorist financing.

As a result of these and other activities, al Qaeda's current and prospective ability to raise and move funds with impunity has been significantly diminished. These efforts have likely made a real impact on al Qaeda's financial picture, and it is undoubtedly a weaker organization as a result.

Indeed, in many respects, the views expressed in the task force's first report are now widely held at home and abroad. But although much work has been done, much work remains.

Although Saudi Arabia has made significant improvements in its legal and regulatory regime, it has not fully implemented its new laws and regulations. Because of that, opportunities for the witting or unwitting financing of terrorism persist.

Indicia of implementation and enforcement are generally unavailable. We are concerned that the unavailability of such indicia may negatively impact the deterrent effect presumably intended by these measures. As our report was going to press, for example, we were unable to find evidence to suggest that the announced High Commission of Oversight of Charities was fully operational. More-

over, its composition, authority, mandate and charter remain unclear, as do important metrics of its likely effectiveness, such as staffing levels, budget, and the training of its personnel.

The mandate and authority of the High Commission of Oversights of Charity is also unclear, relative to that of the Saudi National Entity for Charitable Work Abroad which was first announced in February of this year and which was the subject of a press conference in Washington a few days ago.

At least one other key body, Saudi Arabia's Financial Intelligence Unit, is also not yet fully operational. Reliable, accessible metrics are lacking with respect to many of the other newly announced legal, regulatory and institutional reforms. We find this troubling given the importance of these issues to the national security of the United States.

Additionally, despite the flurry of laws and regulations, we believe that there have been no publicly announced arrests, trials or incarcerations in Saudi Arabia in response to the financing of terrorism. As a result Saudi Arabia has yet to demand personal accountability in its efforts to combat terrorist financing and, more broadly and fundamentally, to delegitimize these activities.

Against its poor historical enforcement record any Saudi actions against financiers of terrorism are welcome. But action taken in the shadows may have little consistent or systemic impact on ingrained social or cultural practices that directly or indirectly threaten the security of the United States.

Not only have there been no publicly announced arrests in Saudi Arabia related to terrorist financing, but key financiers remain free and go unpunished. In sum, we find it regrettable and unacceptable that since September 11, 2001 we know of not a single Saudi donor of funds to terrorist groups who has been publicly punished.

Finally, as Senator Levin indicated, Saudi Arabia continues to export radical extremism. As a core tenet of its foreign-policy, Saudi Arabia funds the global propagation of Wahabism, a brand of Islam that, in some instances, supports militancy by encouraging divisiveness and violent acts against Muslims and non-Muslims alike.

This massive spending is a key part of the terrorist financing problem. We are concerned that it is helping to create the next generation of terrorists and therefore constitutes a paramount strategic threat to the United States.

Saudi Arabia has begun to crack down on domestic extremism, most dramatically through education reform and the banishment or reeducation of scores of radical Wahabi clerics. But our task force found there is little evidence of effective action to curb the ongoing export of extremism.

We have made a number of findings that I hope we can discuss. In the interest of time, however, Mallory Factor will now address the report's recommendations, after which I would be happy to entertain any questions.

Chairman COLLINS. Thank you. Mr. Factor.

TESTIMONY OF MALLORY FACTOR,[1] VICE-CHAIRMAN, INDEPENDENT TASK FORCE ON TERRORISM FINANCING, PRESIDENT OF MALLORY FACTOR, INC

Mr. FACTOR. Madam Chairman, Senator Lieberman, and distinguished Members of the Committee, I am honored to testify here today on the recommendations of the Independent Task Force of the Council on Foreign Relations on Terrorist Financing, of which I serve as Vice-Chair.

This subject is of critical importance to the security of our Nation and the world. Madam Chairman, and Senator Lieberman, I would like to commend you for your interest in and leadership on these very important issues and thank you for inviting us to appear before you today.

I would also like to thank and commend Lee Wolosky for his tireless work and dedication to this project. Achievements of our bipartisan task force are a direct result of Lee Wolosky's dedication to this project and his superior judgment in matters involving this task force.

The Bush Administration has made significant progress in its approach to terror financing since September 11. Our report, which is based on publicly available information as well as discussions with current and former Administration officials, finds that the Administration's effort, combined with those of Saudis and other international partners, has significantly diminished al Qaeda's current and prospective ability to raise and move funds.

Our task force makes the point that there is still much work to be done. It also sets forth a framework of constructive, forward-looking recommendations for improving U.S. efforts against terrorism financing.

We note that Saudi Arabia has also made progress since May 2003 by putting in place new anti-money laundering laws designed to impede the flow of funds from Saudi Arabia to terrorist groups. These laws have a number of exceptions and flaws which would weaken their effectiveness in curbing terror financing if fully implemented.

The real problem is that we could not find evidence of significant enforcement and implementation by Saudi Arabia of several of these new laws. Quite simply, many key financiers of global terror continue to operate, remain free and go unpunished in Saudi Arabia.

Our task force report generally reaffirms the recommendations made in the task force's first report and makes nine new recommendations. Although my written testimony explains each of these recommendations, I will discuss only four recommendations now. However, I welcome the opportunity to discuss any of them in response to your questions.

First, our task force urges U.S. policymakers to build a new framework for U.S.-Saudi relations. We recognize that historically the United States has maintained a policy of noninterference in the domestic affairs of Saudi Arabia. Recently, however, al Qaeda, a terrorist organization rooted in Saudi Arabian domestic affairs, has killed and threatened Americans both at home and abroad. Saudi

[1] The prepared statement of Mr. Factor appears in the Appendix on page 41.

Arabia is now involved in a kind of civil war with extremists. This civil war has global implications.

We propose a new framework for U.S.-Saudi relations which would recognize certain Saudi domestic issues that impact U.S. security. These issues, such as terrorist financing and the global export of Islamic extremism, can no longer be off the table.

We acknowledge that this transition is already underway but our recommendation is still out in front of the Administration's public statements on this issue. We believe that the U.S. Government must engage the Saudis openly and unequivocally to confront the ideological, religious and cultural issues that fuel al Qaeda, its imitators and its financiers throughout the world.

Second, and this was already brought up by Senator Lieberman, we believe that the Executive Branch should formalize its efforts to centralize the coordination of U.S. measures to combat terrorist financing. We commend the Executive Branch for centralizing the coordination of terrorist financing issues in the White House as we recommended in our original task force report. The sound allocation of responsibility to the White House needs to be formalized and, as Senator Lieberman said, institutionalized. And we believe this should be done through a national security presidential directive or some measure similar to that.

Third, we recommend that Congress enact a Treasury-led certification regime specifically on terrorist financing. Many countries have taken steps to improve their anti-money laundering and counterterrorist fighting regimes but many have not. We understand that certification systems should be used sparingly. They can strain relations with foreign governments and require expenditures of resources. The fight against terrorist financing is sufficiently important, however, to warrant its own certification regime. This will ensure that stringent requirements are maintained specifically with respect to foreign nations' policies and practices on terrorist financing.

Such a certification system would require the Executive Branch to submit to Congress on an annual basis a written certification, classified if necessary, detailing the steps that foreign nations have taken to cooperate in United States and international efforts to combat terrorist financing. This would be similar in some ways to the Saudi Arabia Accountability Act of 2003, S. 1888, sponsored by Senator Arlen Specter and co-sponsored by Chairman Collins and others. The Act would provide a good starting point for a terrorist financing certification regime if it were narrowed to focus solely on the financing of terrorism and expanded to apply to other nations.

Sanctions for non-certification could include smart sanctions such as denial of U.S. foreign assistance and limitations on access to the U.S. financial system.

Fourth, we recommend that the National Security Council and the White House Office of Management and Budget conduct a cross-cutting analysis of the budgets of all U.S. Government agencies as they relate to terrorist financing. We believe it is crucial that the U.S. Government keep a central accounting of all financial and human resources expended by the government in combating terrorist financing. We understand this cross-cutting analysis could take a significant amount of work on the part of NSC and OMB.

However, it is crucial for government leaders to gain clarity about who is doing what, how well they are doing, and with what resources.

We commend Jody Myers, a former NSC staffer, for suggesting a similar cross-cutting analysis in his Senate testimony given last month.

I thank you for your time and I look forward to your questions.

Chairman COLLINS. Thank you, Mr. Factor. Mr. Aufhauser.

TESTIMONY OF HON. DAVID D. AUFHAUSER,[1] COUNSEL, WILLIAMS AND CONNOLLY, LLP, FORMER GENERAL COUNSEL, U.S. DEPARTMENT OF THE TREASURY

Mr. AUFHAUSER. Thank you, Madam Chairman.

I just wish I could get back to Maine as often as I have gotten back to this room since I left the government.

Chairman COLLINS. We would welcome you back anytime.

Mr. AUFHAUSER. In early 1996, Osama bin Laden was living in exile in the Sudan. He was at war with the House of Saud policy that countenanced the presence of U.S. military troops on Saudi soil. And he was already plotting mayhem sufficient enough to warrant the establishment of a special issue station at the CIA devoted exclusively to divining his ambitions and his designs. Still, he was largely regarded as the son of a rich man and principally a financier of terror. In fact, the original name for the special-purpose unit at the agency was TFL, Terrorist Financial Links.

It turned out actually that bin Laden was a hapless businessman. His ventures failed and were not the principal source of al Qaeda's wealth. Rather, he tapped something far deeper and more dangerous, hate preached and taught in places of despair, married to rivers of unaccounted for funds that flowed across borders in the counterfeit name of charity and faith. In so doing, bin Laden managed to leverage the tactic of terror into a malevolent dogma embraced by an army of madmen.

How we got here is instructive to where we ought to go next.

In 1974, a disgraced president was driven from office for lies and deceits. In 1977, an international extralegal cartel literally dimmed the lights of the White House, demonstrating profound new powers abroad not tied to guns and bullets. And in 1979, the nadir of U.S. influence—the Shah transformed into a stateless person, hostages held captive for more than a year; a failed rescue mission and the Soviet invasion of Afghanistan.

Tied to that significantly was the takeover of the Grand Mosque in Mecca, challenging the sole claim to legitimacy of the Saudi Royal family as the guardians of the faith. A United States seen as impotent to protect its allies and citizens abroad held little promise to the threatened Saudi monarchy.

So it understandably responded with a vengeance of its own, retaking the mosque and directing an unfathomable wealth of petrodollars—by some estimates that I read while I was still in the Administration north of $75 billion—to demonstrate that it is the true and rightful champion of Islam. It did so by underwriting schools, mosques, call centers, and charities throughout the Islamic dias-

[1] The prepared statement of Mr. Aufhauser appears in the Appendix on page 46.

pora. Wherever there was need they came as teachers, as providers of social welfare and safety nets, and as holy men. But what they taught was unforgiving, intolerant, uncompromising and austere views of a faith that became kindling for Osama bin Laden's match.

At the same time I want to note that there was a parallel explosion in the growth of Gulf and Western State-sponsored NGOs, in Eastern Europe, Africa, the Middle East, and Southeast Asia. Much like the Saudi model of outreach, these organizations rushed in to fill a vacuum left by the abdication of responsibility by sovereign powers to solve issues not uncommon or unlike what we see going on in the Sudan today.

Again through the delivery of default government civilian services of the most basic type—schools, welfare, medical aid—these NGOs, once proud of the principal of neutrality, have become the principal medium of thought and teaching in those areas.

And an air and patina of legitimacy attached to these extralegal, non-sovereign entities and a cover frequently, unwittingly was established to disguise charitable money corrupted for terrorist purposes.

All of these extralegal non-sovereign international entities need more policing, not just of the application of their proceeds, but what they teach and what they preach and the consequence of it. And nowhere is that more telling than when you focus on Saudi Arabia.

It will take a generation, and to be frank a clearheaded program of public diplomacy that, for example, condemns legal sophistries that would justify torture, to recapture hearts and minds poisoned by false teachings of hate. What can be done and should be done to scale back the violence in the interim is to deplete the resources made available to kill innocent people. No tool is more useful in doing so than stopping the funding of terrorism. The Council on Foreign Relations and this Committee are to be commended for the profile given to the subject.

As for al Qaeda, the organization is broken, its central bank severely challenged. Yet today it is more lethal than the day that it brought down the twin towers in Manhattan. It is more a movement than an organization today, less predictable with less explicit design. There are autonomous cells, catering to acts of near nihilism, increasingly funded through pedestrian local criminal activity. And they threaten sudden and senseless death without any purpose. And they do so everywhere today, in Bali, in Istanbul, the London subway system, Casablanca, Baghdad, New York, and Washington.

We know we cannot bunker and guard every school, marketplace, shopping center, airport, train station, or place of worship. So new elements of national power are required to prevent more killing and another calamity. None are more central to the prevention of a calamity than intelligence and the disruption of the lines of logistical support for terror. Money informs and defines both. It informs and defines both with a degree of integrity, reliability, insight, and impact that is without peer.

Many of you have heard me testify before that most of the intelligence and information we get in the war on terrorism is suspect,

the product of treachery, deceit, custodial interrogation, and now we learn the product of torture. But the money records do not lie. They are diaries. They are confessions never intended to see the light of day and they lead to trails of plots not unlike the plot to use ricin in the London subway system which was stopped because of the exploitation of the money trail.

By the way, for those of you who do not know ricin, if made well, is 10 times more lethal than VX gas.

September 11 brought a group of us together in the Administration to tackle the subject of terrorist financing with demonstrable successes. Today there is a new vocabulary about it and it includes new laws, new standards of professional and fiduciary conduct, extraordinary commitments of multilateralism at the UN, World Bank, IMF, and within the G8, 10, and 20, as well as APEC, greater capacity building abroad which I think was alluded to by Senator Lieberman, more sophisticated intelligence and a greatly enhanced partnership with the private sector.

But the effort remains at best a proxy, in my judgment, for the real thing. Terrorism permits murder to masquerade under religious sanction altering the whole DNA of war by placing a premium on the death of women and children. Until it is an act of shame to provide money for any such purpose the blood will flow. Accordingly, we must return to first principles: Terror must be defined, at the UN and elsewhere, in a manner to condemn money intended to kill civilians for political purpose.

We must also disrupt not only the funding of terror but the funding of the teaching of hate because it is the crucible for terror.

And we must address the deficit of hope that haunts much of the Islamic world with debt reduction and meaningful economic aid and development assistance, the very reasons I joined the Treasury Department. Paul O'Neill had a metaphor that I liked, even as quixotic as it sounded, our ambition was to build a well in every village.

Of more immediate purpose within the jurisdiction of this Committee, the assets and cash flow that we seek to freeze and disrupt are located abroad. International cooperation is therefore critical and it requires a new mindset in intelligence that will inform both the nature and the manner of collection.

Our new secrets must be collected with the intention of sharing them and strong enough to withstand a measure of judicial scrutiny abroad. That is a sea change and it is a sea change required by the developing jurisprudence of terrorism and its singular and unprecedented focus on prevention rather than punishment.

In addition, if Madrid has any lessons terrorism funded through criminal activity—and that was the case in Madrid—local law enforcement must be integrated more directly with the national intelligence community to facilitate a two-way dialogue of increasingly equal value.

Finally, we must vest an agency of the U.S. Government with the power to direct and execute the campaign against terrorist financing. The NSC is simply not the appropriate place to direct a theater of war.

The man who straps a bomb to his chest as he enters a marketplace is implacable. He is beyond redemption and cannot be de-

terred. It would be the height of irony and a promise of future tragedy if we permit the orthodoxy of how we have organized ourselves in the past and how we have collected and acted upon intelligence in the past to deter us from responding in the future.

Thank you.

Chairman COLLINS. Thank you for your eloquent statement.

Mr. Wolosky, Mr. Aufhauser mentioned the money trail. The money trail often leads from prominent Saudi individuals to Islamic charities to terrorist groups. That is why the Saudi crackdown and increased regulation of Islamic charities that have been too often used as a conduit to terrorist groups is so important.

However, it appears that some of the Saudi regulations explicitly exempt three of the charities that I mentioned in my opening statement that are alleged to have strong ties to terrorist groups, and that is the International Islamic Relief Organization, the World Assembly of Muslim Youth, and the Muslim World League.

Is there any reason for those three charities to be treated differently from some of the others where the Saudis have, in fact, cracked down? I am thinking, for example, the regulations generally restrict Saudi charities from sending monies overseas and yet those three charities are exempt from that regulation. Is there any reason that they should be treated differently?

Mr. WOLOSKY. That is a very good question and thank you, Senator, for it.

There are issues concerning not only the laws and regulations that have been passed by Saudi Arabia relating to these issues but also their scope and their implementation. The issue that you point out, I believe, relates to this body of law which is the body of law that governs bank accounts that are opened and operated within Saudi financial institutions. And specifically, there is a provision of law 300–1–6–5 which appears on its face to exempt from its purview the three specific organizations that you have identified, which collectively account for billions of dollars in international disbursements, from the body of law of which it is a part and which restricts or prohibits disbursements by Saudi-based charitable institutions abroad.

It is an open question and it is one that I would encourage this Committee to pursue, and certainly our task force will pursue it. But it certainly appears to be a case where the exemption might swallow the rule.

In addition, I would like to point out that there are questions regarding the scope of the purview of the new institutions that are being created to regulate Saudi charities. And in that regard, I note that in a press conference just a few days ago in Washington a new entity was announced into which all Saudi charities were going to be dissolved, at least that is what was indicated by the Saudi spokesperson.

However, when pressed for specific charities he indicated not only Al Haramain, which was a primary focus of the press conference, but a bunch of what I would consider relatively minor organizations, namely the Committee to Support the Afghans, the Committee to Support the Bosnians, the Committee for Relief in Kosovo, the Crossover Relief Fund, and the Committee to Support the Palestinians.

I certainly welcome the inclusion of these organizations within the new entity that has been established to regulate charitable giving abroad but really what was not mentioned were those three multibillion-dollar organizations which are a significant part, and should be in my judgment, a significant part of any overall Saudi efforts to regulate charitable giving abroad.

Chairman COLLINS. Thank you.

Mr. Aufhauser, the money trail often leads back to very high-profile wealthy individuals living freely in Saudi Arabia. In fact, the report notes three prominent men whom the Treasury Department has listed as specifically designated global terrorists, and I believe two of the three were added to that list while you were at the Treasury Department as General Counsel.

In your judgment, why are not Saudi leaders cracking down and arresting and making an example of these prominent individuals who are the source of considerable funding for terrorist groups?

Mr. AUFHAUSER. Let me answer it in a somewhat roundabout way because I think your opening statement alluded to the Joint Terrorism Task Force, about which I was vainly proud at the time I left the Treasury Department, as being a singular success.

The ambition of that task force was to take our body of knowledge of their domestic citizens, including prominent merchants of Jetta or Riyadh and to ally it with, for the first time that I am aware in our history of cooperation with domestic law enforcement compulsory process powers of the Saudi government so that they could take what I will call our package of intelligence and remold it and morph it into a package of evidence sustainable in a court of law and that would permit a judicial action of a criminal nature.

Mind you, they did take the action of freezing assets so they have done the regulatory administrative measures we asked of them with regard to those three miscreants.

The disappointment about the Joint Terrorism Task Force is that it apparently has not been used to date to complement the intelligence that we have shared on those three gentlemen and on others, but rather its resources appear to have been redirected to the forensic demands of the bombings. So we have, with some irony, new zeal in the pursuit of terror in Saudi Arabia but at a substantial cost to less resources devoted to the export of terror.

Chairman COLLINS. Thank you. Senator Lieberman.

Senator LIEBERMAN. Thanks very much, Chairman Collins.

Let me focus on one interesting aspect of your report which is about the failure to use a part of the Patriot Act, Section 311. It gives Treasury anti-money laundering special measures to prosecute terrorist financing in countries with inadequate banking regulations and, in fact, to restrict any bank charity business or country that engages in money laundering from using U.S. markets.

Your report today states that these special prosecutorial powers have still not been used, or perhaps used recently, once against a Syrian bank.

Why is that, and what can we do to get the folks in the Administration and in the Treasury Department, to use these powers more aggressively? Mr. Wolosky or Mr. Aufhauser, whichever one of you would like to answer.

Mr. WOLOSKY. I do not know. I cannot speak to why they have not been used more broadly. As you point out, our first report in October 2002 urges the U.S. Government to use more aggressively the special measures contained in Section 311 of the Patriot Act to prohibit or restrict the access of certain foreign jurisdictions or specific foreign financial institutions from the U.S. financial system under the powers in that act.

Certainly it has been the case that to the extent that you use classified material to support those designations you have to have concerns about challenges to your designations under the Administrative Procedures Act in court in such a way that you might have to reveal the classified information.

Fortunately, there have been changes to the law since the enactment of Section 311 to protect classified information from disclosure. So any historical concerns in that regard that might have existed with respect to the use of this aspect of the Patriot Act, I believe, are mitigated.

Senator LIEBERMAN. What can you tell us about the recent use of Section 311 of the Patriot Act against the Syrian bank? Just briefly.

Mr. WOLOSKY. What I can tell you is that it is the first instance of the use of that provision of the Patriot Act in respect to terrorist financing.

Senator LIEBERMAN. What were the circumstances? Is that publicly available?

Mr. WOLOSKY. Is not publicly—the specific basis for the designation, I do not believe, is in the public record.

Senator LIEBERMAN. Mr. Aufhauser, I want to get you into this discussion based on your previous experience, but I would also begin by raising this question. I presume that Section 311 of the Patriot Act could be used to leverage or compel cooperation from Saudi banks, for instance, by giving them a very strong economic incentive to cooperate or run the risk of losing U.S. business and being unable to do business in the United States.

Mr. AUFHAUSER. Let me give you the benefit of my perspective. First, Lee is right, not laying any responsibility at the door of Congress. It took about 9 months for you all to grant an evidentiary privilege that protected classified information in any Section 311 action.

IEPA gave it to us automatically in freeze orders but not under the Patriot Act. It was one of the first things I asked for but it took a while to wind its way through the uncharted course of Congress.

Second, it is not really fruitful to name and shame a bank as a mere act of political theater. If it does not have substantial correspondent banking relationships with the United States, it is merely political theater. But that informed a lot of judgments about what I will call bad banks, and the Treasury Department does have an informal bad banks initiative going on right now, focusing particularly on banks that are implicated in the export of nuclear materials, the improper export of nuclear materials.

Senator LIEBERMAN. The financing of those exports?

Mr. AUFHAUSER. Trade financing and the like of those exports.

Third, where we thought we had problems with banks, and again this is an important distinction I made earlier with Senator Col-

lins, intelligence is called intelligence because it is not fact. It is inference based on being a truffle hound and digging something up which is suggestive.

We have gone abroad and sought the domestic assistance of countries and regulators to reform suspect banks. It is a better way then merely using the blunderbuss of a nuclear Section 311 action against a bank that does not otherwise maintain correspondent accounts.

Senator LIEBERMAN. So, in other words, it is not worth using because it will not really hurt them because they do not have correspondent relationships with U.S. institutions?

Mr. AUFHAUSER. In many instances, you are talking about rather minor banks that do not have correspondent relationships.

Now the Syrian banks in question do have correspondent relationships with several New York banks. They are modest in scope but the gravimen of the Syrian banks was believed by the Administration to be so grave, particularly—they were the principal conduits for the UN Oil for Food Program frauds, for the smuggling of unsanctioned oil out of Iraq and for using some of those funds or placing them in the hands of Hezbollah.

So it was a very strong case and not withstanding the modest ties with New York banks, it was decided that it should be pursued.

Senator LIEBERMAN. How about the Saudi banks? Do they tend to have correspondent relations with U.S. banks that might bring them within Section 311?

Mr. AUFHAUSER. Yes, and they also have, interestingly, substantial correspondent relationships, even more substantial correspondent relationships, with European banks.

There is an open legal question—I think, frankly, it falls against us, I actually asked my staff to look at it at one juncture—whether the Patriot Act Section 311 permits what I call a secondary boycott. That is if we say a bank in Saudi Arabia, following your hypothetical, is to be barred from correspondent banking in the United States, can we say that any bank that does banking with it abroad is similarly barred? I think the way the act is written now, the answer to that is no.

Senator LIEBERMAN. So, bottom line, you would say that in some cases it does not make sense to use Section 311 of the Patriot Act because the banks do not have correspondent relations here. But, generally, would you counsel that it be used more aggressively?

Mr. AUFHAUSER. I will do more than counsel. I will tell you, in the next calendar year, because of the bad banks initiative that I mentioned, there will be substantial actions taken against miscreant banks under Section 311.

Senator LIEBERMAN. Good. Thank you, my time is up.

Chairman COLLINS. Senator Coleman.

Senator COLEMAN. Thank you. Mr. Aufhauser, in your testimony you noted that if Madrid has any lessons, local law enforcement must be integrated more directly with the national intelligence community to facilitate a two-way dialogue of increasingly equal value. Do you have any specific recommendations as to how we accomplish that?

Mr. AUFHAUSER. Perhaps, but let me build down. One of the questions that you all said you were going to pose here is what are the Treasury Department's equities at the table if you were going to have terrorist financing, one general and one command post and an aggregation of resources.

One of the problems I found at the Treasury Department in pursuing terrorist financing is it was not a fully integrated member the intelligence community. So is was not always made aware of the full panoply of counterterrorism activity and relationship that was going on with any country that I was visiting.

So, as a consequence, you could find yourself across the table from folks who thought they were trading different poker chips and equities about cooperation when I was demanding cooperation for terrorist financing.

As a consequence of that, I pushed, and Secretary Snow pushed, for the creation of an Assistant Secretary for Intelligence so that we could be more integrated into the intelligence community, subject to oversight by the Intelligence Committee here on the Hill.

That was passed by Congress, I think wisely passed, and someone will soon be named to that post.

Obviously something less formal was in the offing for the integration of local law enforcement but getting them to the table with the information that they are developing about the petty crimes that are perhaps tied to terror, and marrying that information with what the Federal Bureau of Investigation and what the CIA is developing, is absolute critical in my judgment.

Madrid was financed with false passports, smuggled aliens, and the sale of hashish, all of it known to the local police and most of it not known to the national intelligence officials. National intelligence officials were aware of activity at the area. If the two had been married, maybe something could have been prevented. It is not unlike the quandary we find the 9/11 Commission facing.

Senator COLEMAN. The challenge we have, though, is how to marry that. I come from a local prosecutor perspective, Attorney General's Office in Minnesota. We have our Joint Task Force now and we seem to be making headway. But both structurally and practically there are barriers. I am looking for practical suggestions on how to overcome those.

Mr. AUFHAUSER. Let me give you one possible vehicle. FinCEN is responsible for the compilation of currency transaction reports and suspicious activity reports. It is all put into a computer and it is all made available by access to local cops, cops in Toledo or cops in Minneapolis. If they have an inquiry about Aufhauser, they can ping the FinCEN database.

That FinCEN database is in the process of also being married, in a more secure sense, with what the agency is developing from abroad. This is also being married, in a more secure sense, with what has been developed by the FBI with regard to intelligence issues, terrorism issues.

If local law enforcement could somehow have classified online access to that kind of information it might materially advance our defense of the Nation.

In addition, this is most important and I am talking to you like a local prosecutor, you guys have to share towards Washington,

too. Because I am finding, from what I am reading and what happened in Madrid, is that the better information was known locally.

Senator COLEMAN. That is very helpful.

I am trying to somehow weigh Mr. Factor's testimony with Mr. Wolosky's. Mr. Factor, you noted what I would say structural changes in the relationship dealing with the Saudis, that if we had a certification regime that would be helpful, that you recommend the Saudi's fully implement new laws and regulations.

The concern I have in terms of dealing with terrorist financing, as does Mr. Wolosky, listening to your testimony, there seems to be a fundamental lack of commitment on the part of the Saudis to actually confront this evil.

Are looking for structural changes enough? Or are we simply changing the shape of the box?

Mr. WOLOSKY. It is a good question. It is a difficult question. Of course, we are reporting to you on the same report, so the fact that our testimonies are somewhat schizophrenic is a reflection of the fact that much has been done, as I said, but much work remains.

As you point out, we do recommend a fundamental change in the nature of the bilateral relationship. As Mallory described, one which is more declaratory and one which focuses—or at least does not put off of the table—issues that historically have been considered purely domestic ones in Saudi Arabia. We have come to the conclusion, as have many Americans and Members of this Committee, that after the murder of 3,000 Americans with respect to issues that implicated domestic Saudi problems and concerns, that those issues can no longer be off of the table.

But your question is a good one. Ultimately, in issues of political will, as we have pointed out in our report and in our testimonies, welcome the aggressive pursuit of al Qaeda cells. We condemn the fact that financiers have not been arrested. Those are different issues. They go to issues in my judgment, and in our report's judgment, of political will.

It is relatively easier to go after people who are socially marginalized, members of cells. It is much more difficult to go after financiers who are members of the economic and political establishment.

Mr. FACTOR. I would add on to that that it may seem schizophrenic but it really is not, it is very consistent. We are calling for a new framework for U.S.-Saudi Arabian relations.

For decades U.S.-Saudi Arabia relations have been built upon a consistent framework well understood by both sides. Saudi Arabia would be a constructive actor with regard to the world's oil and markets and regional security issues. And the United States would help provide for the defense of Saudi Arabia, work to address the Israeli-Palestinian conflict, and not raise any significant questions about Saudi Arabian domestic issues, either publicly or privately.

That has changed. We have to bring these things into the open light of day. We are an open society, they are an opaque society. If you want to change, you need political will to have those changes, as Madam Chairman pointed out.

And we have to work with them to force that issue.

Senator COLEMAN. Thank you, Madam Chairman

Chairman COLLINS. Thank you. Senator Lautenberg.

Senator LAUTENBERG. Thank you, Madam Chairman.

Once again I want to express gratitude for the fact that you are holding this hearing. We have a very good panel of witnesses. Their statements are extremely interesting and I think you have furthered the cause and the fight against terrorism. I greatly respect and appreciate that.

I want to get a couple of things out in public view. Mr. Aufhauser, I am sure you heard about the amendment that we passed, and as I mentioned in my opening remarks, that would shut down subsidiaries, either real or sham, that are then in turn used to do business with rogue states.

Have you been aware in your previous government service or since then that these things exist?

Mr. AUFHAUSER. Yes.

Senator LAUTENBERG. Is it important——

Mr. AUFHAUSER. In a broader context, if I can say. Generally speaking, the economic sanctions laws and OFAC regulations for which I was responsible have enormous loopholes for subsidiary conduct abroad.

Senator LAUTENBERG. So let me extend your comment a little bit and say I take an implication there that we ought to close it down wherever we can do it?

Mr. AUFHAUSER. If you believe in the effectiveness of the economic sanctions programs which are part of our law, yes.

Senator LAUTENBERG. It was disappointing that we lost that amendment by a single vote but that is what happened.

Mr. Wolosky, are we doing enough—and Mr. Factor may have just mentioned—to put public pressure on the Saudis? Do you think that we can ratchet that up substantially for the benefit of the elimination of this financing route that encourages terrorism?

Mr. WOLOSKY. Certainly we can, in some instances, yes. The report recognizes that some issues are best dealt with privately. But it also strongly urges a more declaratory policy when the U.S. Government finds significant and enduring shortcomings in the response of Saudi Arabia to terrorist financing issues.

Benchmarks need to be set out publicly if they are not being met privately. Individuals, who the United States has designated as terrorist financiers and has indicated in no uncertain terms part of the al Qaeda financial network, and who have not been incarcerated in Saudi Arabia, those are the very issues that need to be brought to the fore of our public statements and respect of these matters.

Senator LAUTENBERG. The private discussions do not have the same effect. And I think we ought to declare once and for all that if Saudi Arabia has to dial 911, as they did in 1990, do not call us. The phone is going to be out of order. And that we have to say that every dollar, let the word go out of this Committee and across the media. Let the word go out that if you contribute to anything that encourages terrorism that it is pointing a gun at the head of our people. And we are going to think of it that way and our punishment is going to be swift and full.

It is bothersome as the devil to me that—and I was early on the ground in the Gulf War, and I have been to Iraq since then, and

I know a lot of people associated with the Saudi government and had some semi-friendly relationships with them.

But for them to pass off the blame, it is in print and the news, when the Crown Prince Abdullah statement after the May 24 attack at Yanbu says "Zionism is behind terrorist actions in the kingdom. . . . I am (95%) sure of that." And the Foreign Minister then affirms these comments, says the affirmation of these comments is again absolutely correct, 95 percent. And then Adel Jubeir declined to repudiate these statements at a June 2, 2004 press conference. And the State Department has been silent on them. And they have to speak out.

I think Mr. Aufhauser made a very important statement. He talked about the fact that we have to recognize that this is far beyond the normal activities that we see these oblique apologies, etc. Because it is inherent in the culture. When you teach little kids to hate other little kids, that is the beginning of the end. It is the end of their lives and the end of peaceful lives around the country. And we have to make sure that they understand that in public terms, and denounce that kind of educational thrust. It just is not going to work and it is not helpful.

I would ask one last question here. I know that you have seen the report that was issued in the *New York Times,* on June 12. It talks about some internal dispute within the task force. And perhaps some redaction or reduction in terms of the comments that the task force report was going to carry.

Mr. Factor, I would ask you, you are very much a part of the activities that go on in our government and I say that respectfully, and you are also a businessman that knows very much about how things operate in terms of financing and investor relationships and things of that nature.

So when you see a report issued and it is suggested that you thought maybe this report was too critical, is that the context of the article that was printed in the *New York Times* that suggested there was dissension and some alteration made by you to get this report in acceptable fashion for the Administration, as well as for the mission?

Mr. FACTOR. I can only answer that this report is a consensus report. We all had various beliefs and feelings and we talked those out very thoroughly. Our project directors' position was to try to reach a consensus and try to put together the fairest, most accurate, bipartisan report possible. We believe we have achieved that. And I believe all of us unequivocally support the findings and recommendations in this report and we are very proud of it.

There were many discussions on a host of topics. We solicited information from a host of people—the Administration, Saudi Arabia. We, at one point, planned a trip over there which never came about. It is very common for all task forces at the Council on Foreign Relations to solicit input from the subjects of those task forces. So this is a common thing.

Senator LAUTENBERG. Even after the report is complete, a report is not complete?

Mr. FACTOR. A report is not complete until everybody signs off on it.

Senator LAUTENBERG. Thank you.

Chairman COLLINS. Thank you, Senator.

Mr. Wolosky, before I turn to Senator Specter, I want to give you an opportunity to discuss the issue that was just raised, as well, since you were one of the two principal authors of the report.

Mr. WOLOSKY. Thank you.

First, I would like to respond to another point that Senator Lautenberg made concerning the anti-Semitic statements made by the Crown Prince and consistently reaffirmed by other Saudi officials, including just a few days at a press conference in Washington. In my view, and in the view of our task force, they call into question the commitment of Saudi Arabia as a reliable partner in the war on terror. They cloud its efforts in moral uncertainty. And they must be immediately retracted.

The U.S. Government, the President of the United States, in my view, should immediately condemn those statements and urge the Saudis to condemn those statements.

I personally was very distressed to see a senior State Department official stand by on June 2 in Washington and not repudiate those comments in response to a question from a reporter. In my view, that is a disservice to many people and to the war on terror.

Now as to the *New York Times* report, as I have discussed with your staff, I wish to clarify that the language that was in the first draft of the report I distributed to the full task force membership on May 2, 2004 was as follows: "There is insufficient evidence to conclude Saudi Arabia has fully implemented its new laws and regulations and important questions remain. As part of Saudi Arabia's offer of assistance to the work of our task force, we sought to visit Riyadh to discuss, among other things, the state of the implementation of these new laws, regulations and oversight mechanisms."

Senator LAUTENBERG. Madam Chairman, I appreciate the clarification. Thank you.

Chairman COLLINS. I thought it might be helpful to you, Senator.

Senator LIEBERMAN. Madam Chairman, I join you. Tomorrow morning, when we open our *New York Times*, I expect the headlines to say "Times Snookered."

Chairman COLLINS. Senator Specter.

OPENING STATEMENT OF SENATOR SPECTER

Senator SPECTER. Thank you, Madam Chairman, and thank you for scheduling these hearings.

I compliment the Council on Foreign Relations for undertaking this kind of study. I am very interested in all of your findings.

I focus for just a moment on the one that Saudi Arabia, whose people and organizations contribute 60 percent of the annual budget of Hamas, does not recognize Hamas as a terrorist organization. Mr. Factor or Mr. Wolosky, do you know what their factual basis is for that kind of a statement, when Hamas admittedly target civilians?

Mr. FACTOR. I do not know what their basis is for that. I can only speculate.

Senator SPECTER. Mr. Wolosky.

Mr. WOLOSKY. My own personal view is that one man's terrorist is another man's freedom fighter.

Senator SPECTER. That is a fine generalization of another era, but not when civilians are targeted.

Mr. WOLOSKY. It is not my view, Senator. It is my sense of what the Saudi position on Hamas is. I firmly believe that Hamas is a terrorist organization.

I also think that there is a misconception. David Aufhauser has used the word sophistry in understanding what Hamas is. The sophistry lies in the fact that it is true that Hamas provides social services in Palestinian territories. However, it is also a terrorist organization that kills innocent people. A vast majority of its funds have come from Saudi Arabia in recent years. Only relatively recently has that begun to change at the official level, although private Saudi contributions to Hamas must continue to be strictly monitored.

Our report recommends, in fact it goes very far on this issue, and it recommends that as a mandatory matter of international law, the United Nations Security Council pass a resolution that specifically designates Hamas as a terrorist organization and obligates all member states to close down Hamas organizations and fronts.

Senator SPECTER. Mr. Aufhauser, let me ask you a different question, and that is what more could the Administration do in a very active way to motivate the Saudis or compel the Saudis or sanction the Saudis into doing a better job on fighting terrorism?

Mr. AUFHAUSER. Well, they have come a long way, as you know from testimony I have given before committees that you have sat on, as outlined by Lee and Mallory and the Council. Some extraordinary systemic changes. But what is missing is a sense of personal accountability and follow-through.

Also, on the broader scale, and I think far more important to us, far more important to us than personal accountability of one or two bad actors, is to stop the funding of the teaching of hate. And I think there should be a concerted Administration policy and campaign.

Senator SPECTER. Mr. Factor, thank you for the statement in your opening statement about the Saudi Arabia Accountability Act, which was cosponsored by the Chairman, and I am the principal sponsor, to provide a good starting point for focusing on terrorist financing certification regime.

Mr. Aufhauser, the Administration at first opposed the Syrian Accountability Act and then moved from opposed to neutral. And I think finally ended up perhaps inferentially supportive, although the formal neutral position was never changed.

What do you think the prospects are for the Administration to move to neutral or to support the Saudi Arabia Accountability Act? Or somewhere in between.

Mr. AUFHAUSER. I would just be guessing, Senator, but there is an institutional prejudice, understandable and I think to be lauded, at the Treasury Department to only have economic sanctions programs that are really quite enforceable and with real-world impact. And so they are studied about whether or not what has been proposed can be pursued and whether it can be effective.

Can I just say one thing about Hamas?

Senator SPECTER. Sure.

Mr. AUFHAUSER. It is reprehensible that they are not treated as a terrorist organization by the Saudis, I agree, but some historical perspective helps. For 6 years we have urged our European counterparts to join us in naming Hamas as a terrorist organization. And it was only September of last year that they finally joined us as another school bus was blown up in Jerusalem.

Even now, immediately after the designation of Hamas as a terrorist group by the Europeans, we then went to our European allies and said here are four organizations that are transmitting money directly to Hamas. And we were turned down in the freezing of those assets by all of them because they are still not use to the idea. They still cling to what I said before, the sophistry that the social welfare program of Hamas somehow excuses money that goes to killing.

The recent raids by the Israelis on banks, four banks in the West Bank, and the actual seizure physically of money intended for rejectionist groups, was intended to send a signal to a new funding source of Hamas, and that is Iran and Syria, getting back to your Syrian issue.

And informed intelligence sources tell me that for whatever reason, the money going to Hamas from Saudi Arabia has substantially dried up. Nobody can divine the reason. But it has been supplemented by money from Iran and Syria flowing through even more dangerous rejectionist groups in the West Bank.

Senator SPECTER. Thank you very much. My time has expired. I thank you, Madam Chairwoman.

Chairman COLLINS. Thank you Senator. Senator Pryor.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Thank you, Madam Chairman.

I would like to join all my colleagues on the Committee in thanking you for your leadership on this issue.

If I may follow-up with some of Senator Specter's questions, Mr. Aufhauser, something you said a few moments ago. You said that they need to stop funding the teaching of hate. That is a foreign concept, I think, to us here in America. Could you elaborate on that a little bit and explain to the Committee exactly what you mean by that?

Mr. AUFHAUSER. Sure. Wahabism, which is the strain of Islam that they endorse and champion, is very austere, very severe, very uncompromising and very intolerant of differences in views, and can easily be morphed into religious sanction for violence.

And it is taught by clerics who are sent out globally with funding from the Ministry for Islamic Affairs, which in my judgment is a much more important audience to talk to about our future then the Ministry of Internal Security or Defense in Saudi Arabia.

Indeed, on my last trip to Saudi Arabia, we met with the Minister for Islamic Affairs and he affirmed that they need to do some trimming of their clerical group to weed radical extremists out of it. Unfortunately, their first focus has been domestically and not those who have already been exported abroad.

Senator, one last thing. I had a dinner with the prime minister of one of the Southeast Asian countries who said he will not let an

Islamic cleric into his country anymore. The reason is they teach a hate which becomes a bullet.

Senator PRYOR. Let me follow-up on something you said, that they have focused internally first, within Saudi Arabia. But apparently, there is not much evidence to show that they are trying to curb the export of terrorism and extremism. Is that fair to say, for Saudi Arabia?

Mr. AUFHAUSER. I hope I am not sounding too legalistic—to me, this is a very important thing. I chaired a group in the situation room at the White House every Wednesday morning, and it was a group of terrific men and women from every agency of any relevancy, where we would review what we had learned in the preceding 7 days about terrorist financing.

We had a mountain of evidence about the financing of the teaching of hate, who was funding it, where it was going, what they were teaching in the schools, who the converts were, what social welfare they were pursuing, what the threat was in pursuing something more militant.

And we had a modest pile over here on my right hand which was evidence of the funding of an act of terror.

So there is a distinction between fundamental and extremism and an act of terror that gives us the power to try to act abroad in policing things.

The problem with the Saudi model today is it is a blizzard of this funding for folks who teach people that I am their enemy. There is even something more dramatic—it is not the Saudis, but the Iranians that fund a radio station out of Beirut called al-Manar, to the tune of about $110 million a year. That funding helps al-Manar publish and broadcast every day a screed that says Jews and Americans should be killed.

Now should we not stop that funding of that broadcast?

That is not an act of terror. But it is no different from lighting a match in a parched forest.

Senator PRYOR. I know that you would never speak for any of these countries and you would never presume that, but I would like to get your impressions, if we can focus on Saudi Arabia, on why they have not cracked down internally? I am just assuming there are domestic reasons, domestic political reasons that they may fear a backlash within their own country for doing this. I would like to get your impressions on that.

Mr. AUFHAUSER. The most immediate reason for no activity on terrorist financing is they are singularly focused on the guys who are trying to kill them within their confines. They are not looking for financiers. They are looking for terrorists. If he happens also to be a financier, he is a dead man.

So they are devoting virtually every police and intelligence and military resource they have to ferreting out terrorists within their own cells.

That has drawn away, as I said earlier, ironically the focus that we wanted them to have. I cannot blame them. I will tell you that. But for the moment it has drawn away literally every resource from looking at people who export—I think it was Senator Levin who said Saudi Arabia exports two things, a counterfeit religion and oil. He is only two-thirds right. They also export money.

And that money is the purchase for terror. And we would like them to refocus on that.

Senator PRYOR. Madam Chairman, since I have just a few seconds left, I would like to ask the other two witnesses to respond to that last question about Saudi Arabia. Why, in your impressions—not to speak for them, but your impressions about why they are reluctant to crack down internally or at least why they have not done so to date?

Mr. FACTOR. I believe that they have a civil war on their hands which is their first and foremost interest. They also have not had enormous pressure put on them to open up their society. And they fear for their own regime being toppled. So putting all of those three things together, what is being exported is a secondary issue.

I believe the conclusion they need to come to very rapidly is that that civil war will never be solved as long as they are exporting money that could be used for terrorism.

And last, the political will of the country has to establish that no cause, however legitimate, justifies the use of terror. Indeed, the use of terror delegitimizes even the most worthy cause. They have to build political will on that, which they are not doing doing.

Mr. WOLOSKY. I largely agree with these two comments.

First, I do think they are trying to crack down internally. They are fighting a civil war because it threatens the leadership of their country. It threatens their lives. And they are dedicating resources to fight that civil war.

They are also cracking down internally, at least there are suggestions that they are cracking down internally, on the extremism that is propagated within Saudi Arabia. Our report makes a distinction between the propagation of extremism within Saudi Arabia and its export outside of Saudi Arabia.

Within Saudi Arabia we have seen the remarkable spectacle in the past year, for instance, of clerics, extremist clerics, going on television to renounce their old views. That is a rather remarkable occurrence within the cultural and social context in which it has occurred.

Externally, we find very little evidence of action being taken in respect to this pile, the pile that evidences the flow of billions of dollars in support of the propagation of extremism internationally. And our report says that constitutes, that export of extremism constitutes a strategic threat to the United States.

I think we are the first group to go that far in characterizing that financial flow in that manner.

Senator PRYOR. Thank you, Madam Chairman.

Chairman COLLINS. Thank you.

We have had a vote just called. So I am going to do one final quick round of a question each, and then we will adjourn the hearing. I do thank you for your very valuable testimony.

Mr. Factor, as you know from our discussions, I am particularly interested in the recommendation of the report that we pass legislation creating a certification whereby the President would certify the compliance of nations with an effort to halt terrorism financing.

Some people have expressed concerns that would be too narrow a test for nations to have to pass. They say that the war against

terrorism is a broad war being fought on many fronts and that it would be a mistake to just look at this one factor.

Could you comment on whether you think the separate analysis of compliance with the effort to halt terrorism financing is appropriate? Or should the certification be a broader assessment?

Mr. FACTOR. It is our belief on the task force that the certification should be for terrorist financing. I am not going to suggest that other certifications might not be needed or necessary, or for that matter might be unnecessary. But we believe that if you follow the money, if you check out the money, if you are sure where the money is going and how it is going, you will have the opportunity to cut down on the abilities of terrorists to operate throughout the world. We believe a certification regime specifically on terrorist financing is necessary and called for.

We also believe that we would give waivers to the President obviously and the information can be classified. But we need to name and shame and bring the open light of our society and the discussion that our society allows forward. The only way we will do it is not by getting it confused in a broader regime.

Chairman COLLINS. Thank you. Senator Lieberman.

Senator LIEBERMAN. Thanks very much, Chairman Collins.

I am going to submit a few questions to the witnesses for answers in writing, but I did want to ask this summary question.

In your report in October 2002, this language has already been quoted, you said, "it is worth stating clearly and unambiguously what official U.S. Government spokespersons have not for years, individuals and charities based in Saudi Arabia have been the most important source of funds for al Qaeda and for years Saudi officials have turned a blind eye to this problem."

So, your report and testimony today certainly suggest that maybe the Saudi officials, probably the Saudi officials, are no longer turning a blind eye. But there are problems, as you have documented on how fully they are following through.

So, my baseline question for this report, now June 2004. Would the conclusion of October 2002 be essentially the same, which is that individuals and charities based in Saudi Arabia have been the most important source of funds for al Qaeda and also the other terrorist groups? Or, has that changed?

Mr. WOLOSKY. Historically, of course, that has been true and it has been affirmed.

Senator LIEBERMAN. Is it true today?

Mr. WOLOSKY. It is a difficult analysis because of the more diffuse nature of al Qaeda. Al Qaeda is no longer an organization that has a highly centralized command and control mechanism, and that includes its financial components both input and output. It is a much more diffuse movement.

And also that relates to the issue of propagation of extremism which we in this report—again, I think for the first time, although it certainly was implicit in the response of the U.S. Government that David described—are saying is a key part of the terrorist financing problem.

Senator LIEBERMAN. I think that is a very important point today. It is not that we do not know about the export of extremism, but you are saying that while they may have curtailed the funding to

some extent, or at least not turned a blind eye to it, as long as they continue to export extremism then there is trouble.

Mr. Factor or Mr. Aufhauser, do you want to add anything to that?

Mr. FACTOR. I would like to add that we know very well that, for example, the Muslim World League, IIRO, the International Islamic Relief Organization, and the World Assembly of Muslim Youth, known by the acronym WAMY, still operates.

I believe funding to al Qaeda has been stopped to a significant extent. But there is funding to numerous other organizations and other organizations may be picking up what al Qaeda was doing, in terms of operations.

Mr. AUFHAUSER. Can I add one thing? I want to put a spotlight on a reservation put at the front of the Committee's report, which is that you can become Saudi-centric when you talk about terrorist financing and it is a grave danger. They have done remarkable things and they should be given credit for it. There remain substantial issues in Saudi Arabia.

But all that I learned before I left and what I have learned since I left suggest that terrorist financing is alive and well from Iran and Syria and increasingly local criminal activity, and also substantial amounts flowing into the occupied territories from Western Europe still.

I would suggest that the spotlight be shifted, if there is only one spotlight, on what is the more immediate threat right now to homeland security here and to security in the Middle East, which I think is money from other sources.

Senator LIEBERMAN. Thank you, very much. You have done a great public service here and I thank you for it.

Chairman COLLINS. Thank you, Senator Lieberman, for your leadership on this issue and your participation in the Committee's ongoing work examining the sources of terrorism financing.

I want to thank all three of our witnesses today. You have done remarkable work. We appreciate your expertise and your sharing your wisdom and knowledge with the Committee.

The hearing record will remain open for 15 days for the submission of any additional questions. We would ask you to return those as quickly as you can.

I also want to thank our staff for their work on this important hearing. The hearing is now adjourned.

[Whereupon, at 12:29 p.m., the hearing was concluded.]

APPENDIX

PREPARED STATEMENT OF SENATOR GEORGE V. VOINOVICH

Good morning. I would like to thank the Chairman, Senator Collins, for convening this hearing today to examine an issue that is extremely important to our national security—our progress in efforts to deny terrorists the resources they seek to perform deadly attacks against Americans and our allies at home and abroad.

The tragic events of September 11, 2001 brought home to all of us the urgent need to cut off funding for terrorist organizations such as al Qaeda. More than 2½ years later, it is imperative that we continue to make this a top priority of the U.S. Government. Simply stated, we cannot afford to be complacent in our efforts.

Last month, Attorney General John Ashcroft and Secretary of Homeland Security Tom Ridge reminded the American people of al Qaeda's unrelenting desire to again attack Americans on U.S. soil. The potential impact is not limited to those living in our country's largest cities. Just yesterday, Federal officials unsealed an indictment against a Somali man living in Columbus, Ohio. The charges against this man include conspiring with al Qaeda to blow up a shopping mall in Ohio's capital city. This is a chilling reminder of what is possible, and again underscores the need to redouble our efforts to deny terrorists the financial resources that they desire.

Today, an Independent Task Force on Terrorist Financing sponsored by the Council on Foreign Relations will release its second report on our progress in this effort. We are glad to have two individuals who serve on this task force, Lee Wolosky and Mallory Factor, with us this morning. I look forward to hearing their thoughts on how we can step up our efforts at home to disrupt and destroy the financial network of al Qaeda and other terrorist organizations. I also look forward to their views on how we can enhance cooperation with other countries to deny terrorists the funding that they seek—particularly Saudi Arabia.

I would also like to welcome David Aufhauser, who served as former General Counsel at the U.S. Department of Treasury. I look forward to his candid views on how we are doing in this effort here at home, where the men and women at the Treasury Department and other Federal, State and local agencies serve on the front lines in the effort to disrupt and destroy terrorists' financial networks.

As my colleagues are aware, since 1999, I have worked to express the urgency of the Federal Government's human capital challenges and their impact on critically important government functions, such as national security. With strong bi-partisan support from this Committee, I have championed a series of legislative reforms in Congress, which should have a significant impact on the way the Federal Government manages its people in the coming years.

In March 2001, the Subcommittee on Oversight of Government Management held a hearing entitled, "National Security Implications of the Human Capital Crisis." Our panel of distinguished witnesses included former Defense Secretary James Schlesinger, member of the U.S. Commission on National Security in the 21st Century. Secretary Schlesinger discussed a comprehensive evaluation on national security strategy and structure that was undertaken by the Commission. Regarding human capital, the Commission's final report concluded:

"As it enters the 21st Century, the United States finds itself on the brink of an unprecedented crisis of competence in government. The maintenance of American power in the world depends on the quality of U.S. Government personnel, civil and military, at all levels. We must take immediate action in the personnel area to ensure that the United States can meet future challenges."

Secretary Schlesinger added further: ". . . it is the Commission's view that fixing the personnel problem is a precondition for fixing virtually everything else that needs repair in the institutional edifice of U.S. national security policy."

This remains true as our government looks to deny terrorists, whose purpose is to inflict grave harm on the United States, the resources that they seek. I again thank Chairman Collins for convening this hearing, and I look forward to the testimony of our witnesses.

Testimony Concerning the Second Report of an Independent Task Force on Terrorist Financing Sponsored by the Council on Foreign Relations
Lee S. Wolosky, Co-Director
Of Counsel, Boies, Schiller & Flexner LLP
Adjunct Professor, Columbia University
U.S. Senate Committee on Governmental Affairs
June 15, 2004

Madame Chairman, Senator Lieberman and Distinguished Members of the Committee:

Thank you for your dedicated leadership on these issues. This Committee's sustained attention to terrorist financing issues is critically important to our nation.

We are honored to report to you today on the second report of the Independent Task Force Relations on Terrorist Financing sponsored by the Council on Foreign. I have served as co-Director of this bipartisan initiative since its inception in the summer of 2002.

Our report is the result of the hard work of a number of dedicated individuals of both political parties who seek to further vital national interests. I wish to thank our Chairman, Maurice Greenberg, for his unwavering support of the Task Force and his broader leadership in assuring continued attention to, and scholarship on, issues at the intersection of global finance and national security. Our Vice-Chairman, Mallory Factor, undertook important efforts to advance the mission of the Task Force. My co-Director and co-author, William F. Wechsler, brought not only a wealth of talent and energy but the wealth of experience that comes from being the first senior U.S. official to focus seriously on these issues, beginning in 1998.

I am also grateful to Council President Richard Haass. This Task Force would not have succeeded without his support and assistance.

Finally, it is my honor to testify beside David Aufhauser, who served our country with dedication and distinction. Many of the positive developments in this area since 9/11 are the direct fruits of his vision and leadership.

I will discuss the background of our second report and its findings. Mallory will then discuss the report's recommendations. Since the report, along with its various appendices, is almost 300 pages in length, we will only be able to highlight core points. We ask that the full report and its appendices be placed into the record, and we look forward to a fuller discussion of various aspects of the report in response to your questions.

In our first report, released in October 2002, we concluded: "It is worth stating clearly and unambiguously what official U.S. government spokespersons have not: For years, individuals and charities based in Saudi Arabia have been the most important source of

funds for al-Qaeda; and for years, Saudi officials have turned a blind eye to this problem." We recommended the encouragement of the Saudi regime to strengthen significantly its efforts to combat terrorist financing. In this regard, we noted a recent historical record of inattention, denial, and half measures. And we urged the U.S. Government to confront directly the lack of political will in Saudi Arabia and elsewhere through the institution of a declaratory policy that would permit or compel U.S. officials to speak more frankly about the nature of the problem.

The reaction to the release of the Task Force's initial report was reflective of then-prevailing mindsets. The Saudi Arabian Foreign Minister, Prince Saud al-Faisal, told CNN that the report was "long on accusation and short on documented proof." The Saudi ambassador to the United States, Prince Bandar bin Sultan, said the Task Force report was based on "false and inconclusive information" and "clearly out of touch with current activities." He also maintained that "Saudi Arabia has put into place the tools, resources, laws, and regulations to combat terrorism and terrorist financing" and promised to "prosecute the guilty to the fullest extent of the law." The U.S. Treasury Department's spokesperson called the report "seriously flawed."

During 2002 and into the first few months of 2003, U.S. officials quietly engaged their Saudi counterparts on a sustained basis in Washington and Riyadh—at increasingly high levels, with more intelligence they were prepared to share, and with more aggressive demands. Results were mixed. Less transparent methods of curtailing terrorist financing were also stepped up, with significant successes.

The status quo changed on May 12, 2003, when al-Qaeda bombed housing compounds in Riyadh used by U.S. and other foreign residents, prompting more comprehensive Saudi action against terrorism. Public statements and actions by both the United States and Saudi Arabia since May 2003 have evidenced in many respects a more urgent approach to terrorist financing, one that is broadly consistent with our initial report's conclusions, findings, and recommendations.

For example, Saudi Arabia has announced a profusion of new laws, regulations, and institutions regarding money laundering, charitable oversight, and the supervision of the formal and informal financial services sector. Significantly, the government also took steps to remove donation boxes from mosques and shopping malls. And, for the first time, Saudi Arabia has subjected aspects of its anti-money laundering regime to international scrutiny.

While Saudi officials were previously unwilling to acknowledge or address the role government-sanctioned religious messages play in supporting militant Islamic groups, following the May terrorist attacks Saudi officials began to take steps to address the mindset that foments and justifies acts of terrorism.

Most critically, for the first time, the Saudi government decided to use force to hunt—and kill—members of domestic al-Qaeda cells, including, in one case, a financier named

Yousif Salih Fahad Al-Ayeeri (aka "Swift Sword"). Actions on this scale were not in evidence prior to the 2003 bombings.

Saudi Arabia has markedly increased its tactical law enforcement and intelligence cooperation with the United States and the Bush administration acted quickly to take advantage of newfound political will in Saudi Arabia to renew and reinvigorate its own efforts to combat terrorist financing.

The Bush administration also moved toward a more declaratory policy. On June 26, 2003, for example, at the annual U.S.-EU Summit, President Bush took the important step of publicly urging European leaders to criminalize all fundraising by Hamas. That same day, David Aufhauser testified before Congress that "in many ways, [Saudi Arabia] is the epicenter" of the financing of al-Qaeda and other terrorist movements.

The pace of joint U.S.-Saudi designations quickened, specifically in respect to efforts to close problematic overseas branches of the sprawling, Saudi-based Al Haramain Islamic Foundation, which Saudi officials estimate was, at its height, raising between forty and fifty million dollars per year.

As our report was going to press, the government of Saudi Arabia announced the dissolution of Al Haramain and other charitable entities and the creation of a nongovernmental organization to coordinate private Saudi charitable giving abroad.

As a result of the foregoing activities, al-Qaeda's current and prospective ability to raise and move funds with impunity has been significantly diminished. These efforts have likely made a real impact on al-Qaeda's financial picture, and it is undoubtedly a weaker organization as a result.

Indeed, in many respects, the views expressed in the Task Force's first report are now widely held, at home and abroad. But although much work has been done, much work remains.

I will now describe a number of our core findings.

Although Saudi Arabia has made significant improvements in its legal and regulatory regime, it has not fully implemented its new laws and regulations, and because of that, opportunities for the witting or unwitting financing of terrorism persist.

Indicia of implementation and enforcement are generally unavailable. We are concerned that the unavailability of such indicia may negatively impact the deterrent effect presumably intended by these measures.

As our report was going to press, for example, we were unable to find evidence to suggest that the announced High Commission of Oversight of Charities was fully operational. Moreover, its composition, authority, mandate, and charter remain unclear, as do important metrics of its likely effectiveness, such as staffing levels, budget, and

personnel training. The mandate and authority of the High Commission of Oversight of Charities is also unclear relative to that of the Saudi National Entity for Charitable Work Abroad, which was first announced in February 2004. As Juan Zarate told Congress earlier this spring, "the Kingdom must move forward to clarify and empower an oversight authority that will administer effective control over the [charity] sector and ensure compliance with obligations under the new regulatory measures." More recently, on June 2, 2004, Zarate called the establishment of the Saudi National Entity for Charitable Work Abroad a "major step forward" and noted, "we're looking forward to seeing the implementation of that."

At least one other key body, Saudi Arabia's Financial Intelligence Unit (FIU), is also not yet fully functional. FIU's are intended to collect and analyze suspicious financial data. Reliable, accessible metrics are lacking with respect to many of the other newly announced legal, regulatory, and institutional reforms. Critical data necessary to assess the implementation, enforcement, and effectiveness of many of these announced reforms are generally nonexistent or not publicly available. We find this troubling given the importance of these issues to the national security interests of the United States and other countries (including Saudi Arabia) that remain targets of al-Qaeda and similar terrorist organizations.

Additionally, we have found no evidence that Saudi Arabia has taken public punitive actions against any individual for financing terror. As a result, Saudi Arabia has yet to demand personal accountability in its efforts to combat terrorist financing and, more broadly and fundamentally, to de-legitimize these activities. The lack of transparent and compelling evidence of implementation is particularly troublesome in the criminal law enforcement context. Despite the flurry of laws and regulations, we believe that there have been no publicly announced arrests, trials, or incarcerations in Saudi Arabia in response to the financing of terrorism—despite the fact that such arrests and other punitive steps have reportedly taken place.

Against its poor historical enforcement record, any Saudi actions against financiers of terror are welcome. But actions taken in the shadows may have little consistent or systemic impact on ingrained social or cultural practices that directly or indirectly threaten the security of the United States.

Put simply, our Task Force found that people and organizations need to be publicly punished, including for past involvement in terrorist financing activities.

Not only have there been no publicly announced arrests in Saudi Arabia related to terrorist financing, but key financiers remain free or go unpunished. For example, Yasin al-Qadi, a Specially Designated Global Terrorist, appears to live freely in Saudi Arabia. According to the Treasury Department, "He heads the Saudi-based Muwafaq Foundation. Muwafaq is an al-Qaeda front that receives funding from wealthy Saudi businessmen. Blessed Relief is the English translation. Saudi businessmen have been transferring millions of dollars to bin Laden through Blessed Relief." Wa'el Julaidan, who was jointly designated on September 6, 2002, by the governments of the United States and Saudi

Arabia as "an associate of Usama bin Laden and a supporter of al-Qa'ida terror," also appears to live freely in Saudi Arabia. According to the Treasury Department, "The United States has credible information that Wa'el Hamza Julaidan is an associate of Usama bin Laden and several of bin Laden's close lieutenants. Julaidan has directed organizations that have provided financial and logistical support to al-Qa'ida." The same is true for Aqeel Abdulaziz Al-Aqil, the founder and long-time leader of the Al Haramain Islamic Foundation (AHF). According to the Treasury Department, "As AHF's founder and leader, Al-Aqil controlled AHF and was responsible for all AHF activities, including its support for terrorism.... Under Al Aqil's leadership of AHF, numerous AHF field offices and representatives operating throughout Africa, Asia, Europe and North America appeared to be providing financial and material support to the al-Qa'ida network. Terrorist organizations designated by the U.S. including Jemmah Islammiya, Al-Ittihad Al-Islamiya, Egyptian Islamic Jihad, HAMAS, and Lashkar E-Taibah received funding from AHF and used AHF as a front for fundraising and operational activities."

We find it regrettable and unacceptable that *since September 11, 2001, we know of not a single Saudi donor of funds to terrorist groups who has been publicly punished*—despite Ambassador Bandar's assertion, in response to the issuance of our first report, that Saudi Arabia would "prosecute the guilty to the fullest extent of the law."

Finally, Saudi Arabia continues to export radical extremism. A battle of ideas undergirds the global war on terrorism. Militant groups such as al-Qaeda are fueled by uncompromising fundamentalist interpretations of Islam that espouse violence and that millions of Muslims join Christians and Jews in rejecting.

As a core tenet of its foreign policy, Saudi Arabia funds the global propagation of Wahabism, a brand of Islam that, in some instances, supports militancy by encouraging divisiveness and violent acts against Muslims and non-Muslims alike. We are concerned that this massive spending is helping to create the next generation of terrorists and therefore constitutes a paramount strategic threat to the United States. Through the support for *madrassas*, mosques, cultural centers, hospitals, and other institutions, and the training and export of radical clerics to populate these outposts, Saudi Arabia has spent what could amount to hundreds of millions of dollars around the world financing extremism. Such Saudi financing is contributing significantly to the radicalization of millions of Muslims in places ranging from Pakistan to Indonesia to Nigeria to the United States. Foreign funding of extremist *madrassas* in Pakistan alone, for example, is estimated in the tens of millions, much of it historically from Saudi Arabia.

Saudi Arabia has begun to crack down on *domestic* extremism, most dramatically through education reform and the banishment or "re-education" of scores of radical Wahabi clerics. But our Task Force found that there is less evidence of effective action to curb the ongoing *export* of extremism.

Although the United States is not and should not be at war with any religion or any religious sect, we found that U.S. policy should affirmatively seek to drain the ideological breeding grounds of Islamic extremism, financially and otherwise. To do so, we will need more demonstrable cooperation from Saudi Arabia, which so far as not been sufficiently forthcoming.

We have made a number of other findings that I hope we can discuss. In the interest of time, Mallory will now address the report's recommendations, after which time I would be happy to answer any questions.

Testimony Concerning the Second Report of an Independent Task Force on Terrorist Financing Sponsored by the Council on Foreign Relations
Mallory Factor, Vice-Chair
Chairman, MALLORY FACTOR INC
U.S. Senate Committee on Governmental Affairs
June 15, 2004

Madame Chairman, Senator Lieberman and Distinguished Members of the Committee:

I am honored to testify here today to report to you on the recommendations of the Independent Task Force of the Council on Foreign Relations on Terrorist Financing, of which I have served as Vice-Chair.

Madame Chairman and Senator Lieberman, I would like to commend you for your unwavering commitment to these issues. The work this Committee is undertaking is of critical importance to the United States and the world. Thank you for your important leadership.

Until relatively recently, too little was done to curb the flow of funds to terrorists and extremists. That is why the Council on Foreign Relations sponsored this Task Force in 2002 and renewed its mandate more recently. I would like to thank Council President Richard Haass for all that he has done to make this Task Force a success.

Our distinguished bi-partisan Task Force is chaired by Maurice R. Greenberg and directed by William F. Wechsler and Lee S. Wolosky. They led this Task Force in the interest of serving our nation. I believe they have succeeded.

I would particularly like to commend Lee Wolosky, without whose leadership, judgment, diplomacy, draftsmanship and dedicated efforts this task force would not have been a success. Lee worked tirelessly to reach consensus among task force members on the report and its recommendations.

The Bush administration has accomplished a great deal since 9/11. Some of the Administration's achievements in this area have been integrating terrorist financing into the U.S. government's overall counterterrorism effort, securing unprecedented international support for UN sanctions against al-Qaeda, strengthening international standards for financial supervision through FATF, issuing significant and meaningful regulations under the Patriot Act and implementing a wide-ranging strategy to engage Saudi Arabia on the subject of financial and ideological support of extremists. Still, there is much work to be done and I believe that the Task Force report sets forth a framework of constructive, forward looking recommendations for improving U.S. efforts against terrorism financing.

Our report focuses on terror financing from within the Kingdom of Saudi Arabia because of the enormous resources emanating from that state that fund terrorist activities.

Clearly, there are numerous other states that finance terror and that should be examined also.

The Kingdom of Saudi Arabia has accomplished a great deal since May 2003. Most notably, Saudi Arabia has enacted extensive laws and regulations which, if fully implemented, would significantly reduce the flow of funds from within Saudi Arabia to terrorists. However, we have not found Saudi Arabia to be effectively enforcing these laws and regulations as Lee Wolosky has discussed. Many issues still need to be addressed before Saudi Arabia will have an acceptable regime in place to combat terror financing.

Our task force report generally reaffirms the recommendations made in the Task Force's first report and makes nine new recommendations. I will discuss them in varying levels of detail and would welcome the opportunity to discuss any of them in greater length in response to your questions.

First, we urge U.S. policymakers to build a new framework for U.S.-Saudi relations. We recognize the broader context of the complex and important bilateral relationship in which the terrorist financing issue is situated. For decades, U.S.-Saudi Arabia relations have been built upon a consistent framework understood by both sides: Saudi Arabia would be a constructive actor with regard to the world's oil markets and regional security issues, and the United States would help provide for the defense of Saudi Arabia, work to address the Israeli-Palestinian conflict, and not raise any significant questions about Saudi Arabian domestic issues, either publicly or privately.

More recently however, this framework has come under strain because al-Qaeda, a terrorist organization rooted in issues central to Saudi Arabian domestic affairs, has murdered thousands of Americans. Al-Qaeda and similar organizations continue to conspire to kill even more Americans and to threaten our way of life.

Changed circumstances require a new policy framework for U.S.-Saudi relations. When domestic Saudi problems threaten Americans at home and abroad, the U.S. must pay attention to those Saudi "domestic" issues that impact U.S. security such as terrorist financing and the global export of Islamic extremism. These issues can no longer be "off the table"; they must be front and center in our bilateral relationship.

We acknowledge that this transition is already well underway, as evidenced by the turbulence in the bilateral relationship since 9/11. We note that some Bush administration officials have privately characterized the current state of affairs in Saudi Arabia as a "civil war" and suggested that the appropriate objective for U.S. policy in this context is to help the current regime prevail. We agree, but we believe the domestic Saudi problem will not be solved by dispersing al-Qaeda cells and members in Saudi Arabia alone. Rather, the "civil war" will be won only when the regime confronts directly and unequivocally addresses the ideological, religious, social, and cultural realities that fuel al-Qaeda, its imitators, and its financiers all over the world.

Second, we recommend that Saudi Arabia fully implement its new laws and regulations and take additional steps to further improve its efforts to combat terrorist financing. In addition to implementing its recently enacted laws and regulations in this area, Saudi Arabia should also deter the financing of terrorism by publicly punishing those Saudi individuals and organizations that have funded terrorist organizations. It should increase the financial transparency and programmatic verification of its global charities and publicly release audit reports of those charities. Saudi Arabia should also ratify and implement treaties that create binding international legal obligations relating to combating money laundering and terrorist financing.

Third, we suggest that multilateral initiatives be better coordinated, appropriately funded, and invested with clear punitive authorities. The need for a new international organization specializing in terrorist financing issues, as recommended by our initial report, has diminished as a result of significant efforts being undertaken by a variety of international actors. The need for proper coordination and clearer mandates has increased for the same reason. It is now time to minimize duplicative efforts and reallocate resources to the most effective and appropriate lead organization.

Fourth, we believe that the executive branch should formalize its efforts to centralize the coordination of U.S. measures to combat terrorist financing. Our understanding is that, in practice, responsibilities for the coordination of terrorist financing issues have shifted from the Treasury Department to the White House, as we recommended in our original Task Force report. I commend the Bush Administration for this action. However, we believe that this allocation of responsibility to the White House needs to be formalized through a National Security Presidential Directive (NSPD) or otherwise.

Fifth, we recommend that Congress enact a Treasury-led certification regime specifically on terrorist financing. The financial support for terrorism is the life-blood of global terrorism and requires its own certification regime. A separate certification process will ensure that stringent requirements are maintained specifically with respect to a nation's policies and practices on terrorist financing without consideration of other issues.

I believe that the Saudi Arabia Accountability Act of 2003, S. 1888, sponsored by Senator Arlen Specter and co-sponsored by Chairman Collins and others would provide a good starting point for a terrorist financing certification regime if it were narrowed to focus solely on the financing of terrorism and expanded to apply to other nations.

We understand that certification regimes are generally disfavored by the executive branch (which must implement them) and favored by the legislative branch (which they empower). Although controversial, they also have the ability to galvanize quickly action consistent with U.S. interests. Moreover, they require official findings of fact that have the effect of promoting transparency and compelling sustained U.S. attention to important topics that, on occasion, U.S. officials find it more expedient to avoid.

For these reasons, we believe that Congress should pass and the President should sign legislation requiring the executive branch to submit to Congress on an annual basis a written certification (classified if necessary) detailing the steps that foreign nations have taken to cooperate in U.S. and international efforts to combat terrorist financing. We suggest that in the absence of a presidential national security waiver, states that do not receive this certification would be subject to sanctions--including denial of U.S. foreign assistance monies and limitations on access to the U.S. financial system.

Sixth, we urge the U.N. Security Council to broaden the scope of the U.N.'s al-Qaeda and Taliban Sanctions Committee. The UN Security Council should specifically impose international sanctions on other groups and individuals that have been designated as terrorists, as Hamas has been by the United States and E.U. Furthermore, it should require, as a matter of international law, that member states take enforcement action against groups, persons and entities designated by the Sanctions Committee. The enabling resolution for these expanded authorities should explicitly reject the notion that acts of terror may be legitimized by the charitable activities or political motivations of the perpetrator. No cause, however legitimate, justifies the use of terror; indeed, the use of terror delegitimizes even the most worthy causes.

Seventh, we suggest that the U.S. government increase sharing of information with the financial services sector as permitted by Section 314 of the USA PATRIOT ACT so that this sector can cooperate more effectively with the U.S. government in identifying incidences of terror financing. International financial institutions subject to U.S. jurisdiction are among our best sources of raw financial intelligence to identify terror financing, but these institutions need to be given appropriate information from the U.S. government on what to look for. Currently, the procedures required by Section 314 of the Patriot Act which are designed to promote cooperation with financial institutions in identifying terror financing are not working as effectively as they might. We suggest greater information sharing between the U.S. government and the financial institutions within the framework of the Patriot Act in order to allow these institutions to cooperate more effectively with the U.S. government in identifying incidences of terror financing.

Eighth, we recommend that the National Security Council (NSC) and the White House Office of Management and Budget (OMB) conduct a cross-cutting analysis of the budgets of all U.S. government agencies as they relate to terrorist financing. We understand this recommendation is difficult to implement; however, we think that monitoring the financial and human resources that are actually devoted to the various tasks involved in combating terrorist financing will facilitate fully informed, strategic decisions about whether resource allocations are optimal or functions are duplicative. For this reason, the NSC and OMB should conduct a cross-cutting analysis of all agencies' budgets in this area, to gain clarity about who is doing what, how well, and with what resources. Only with such a cross-cut in hand can we can begin to make assessments regarding the efficiency of our existing efforts and the adequacy of appropriations relative to the threat. We commend Jody Myers, the former NSC staffer, for suggesting a similar cross-cutting analysis in his Senate testimony given last month.

Ninth, we urge the U.S. government and private foundations, universities, and think tanks to increase efforts to understand the strategic threat posed to the United States by radical Islamic militancy, including specifically the methods and modalities of its financing and global propagation. At the dawn of the Cold War, the U.S. government and U.S. nongovernmental organizations committed substantial public and philanthropic resources to endow Soviet studies programs across the United States. The purpose of these efforts was to increase the level of understanding in this country of the profound strategic threat posed to the United States by Soviet Communism. A similar undertaking is now needed to understand adequately the threat posed to the United States by radical Islamic militancy, along with its causes, which we believe constitutes the greatest strategic threat to the United States at the dawn of this new century. To be commensurate with the threat, much more will need to be done, not only in Washington, but also by private U.S. foundations, universities, and think tanks, in a more sustained, deliberate, and well-financed manner than that afforded through ad hoc initiatives such as our Task Force.

I look forward to your questions.

Opening Statement of
David D. Aufhauser, former General Counsel,
U.S. Department of the Treasury,
Senior Fellow, Center for Strategic & International Studies
Before the Senate Governmental Affairs Committee
June 15, 2004

In early 1996, Usama Bin Laden was living in exile in the Sudan. He was at war with a House of Saud policy that countenanced the presence of U.S. troops on Saudi soil. And he was already plotting mayhem sufficient enough to warrant the establishment of a special "Issue Station" at the CIA devoted exclusively to divining his ambitions and designs. Still, he was regarded as the son of a rich man and principally a financier of terror. In fact, the original name for the special purpose unit at the agency was "TFL" -- terrorist financial links.

It turned out that Bin Laden was actually a hapless businessman. His ventures failed and were **not** the principal source of Al Qaeda's wealth. Rather, he tapped something far deeper and more dangerous – hate preached and taught in places of despair, married to rivers of unaccounted for funds that flowed across borders in the counterfeit name of charity and faith. And in so doing, Bin Laden managed to leverage the **tactic** of terror into a malevolent **dogma** embraced by an army of madmen.

How we got here is instructive to where we must go.

In 1974, a disgraced President was driven from office for lies and deceits. In 1977, an international extra-legal cartel literally dimmed the lights of the White House, demonstrating profound new powers abroad not tied to guns, bullets or boots on the ground. And in 1979, the nadir of U.S. influence – the Shah transformed into a stateless person; hostages held captive for more than a year; a failed rescue mission; and the Soviet invasion of Afghanistan.

Tied to that was the takeover of the Grand Mosque in Mecca, challenging the sole claim to legitimacy of the Saudi royal family as the guardians of the faith. A U.S. impotent to protect its allies and citizens abroad held little promise to the threatened Saudi monarchy. So it understandably responded with a vengeance, retaking the Mosque and directing an unfathomable wealth of petrodollars – by some estimates, north of $75 billion – to demonstrate that it is the true and rightful champion of Islam. It did so by underwriting schools, mosques, call center and charities throughout the Islamic Diaspora. Wherever there was need, they came as teachers, as providers of social welfare, and as holy men. But what they taught was an unforgiving, intolerant, uncompromising and austere view of the faith that became kindling for Usama Bin Laden's match.

It will take a generation – and a clear headed program of public diplomacy that, for example, condemns legal sophistries that justify torture – to recapture hearts and minds poisoned by false teachings of hate. What can be done and

should be done to scale back the violence in the interim is to deplete the resources made available to kill innocents. No tool is more useful in doing so than in stopping the funding of terrorism. The Council on Foreign Relations, and this Committee, are to be commended for the profile given to the subject.

As for al-Qaeda, the organization is broken, its central bank severely challenged. Yet, today, it is more lethal than the day that it brought down the twin towers in Manhattan – more a movement than an organization with predictable or explicit design. Autonomous cells, catering to acts of nihilism, increasingly funded through pedestrian criminal activity, threaten sudden and senseless death without purpose. And they do so everywhere – Bali, Istanbul, the London subway system, Casablanca, Baghdad, New York and Washington. We cannot bunker and guard every school, marketplace, shopping center, airport, train station or place of worship.

New elements of national power are therefore required to **prevent** the killing. None are more central than intelligence and the disruption of the lines of logistical support. Money informs and defines both with a degree of integrity, reliability, insight and impact that is without peer.

9/11 brought a group of us together in the Administration that tackled the subject with demonstrable successes. Today, there is a new vocabulary about

terrorist financing and it includes new laws, new standards of professional and fiduciary conduct, extraordinary commitments of multilateralism at the UN, World Bank, IMF, and within the G8, 10 and 20 as well as APEC, greater capacity abroad, more sophisticated intelligence, and a greatly enhanced partnership with the private sector.

But the effort remains, at best, a proxy for the real thing. Terrorism permits murder to masquerade under religious sanction, altering the whole DNA of war by placing a premium on the death of women and children. Until it is an **act of shame** to provide money for any such counterfeit purpose, the blood will flow. Accordingly, we must return to first principles:

- Terror must be defined -- at the UN and elsewhere -- to condemn money intended to kill civilians for political reason;
- We must disrupt the funding not only of terror, but of the teaching of hate that is its crucible; and
- We must address the deficit of hope that haunts much of the Islamic world with debt reduction and meaningful economic aide and development assistance. Paul O'Neill and I had a metaphor for that proposition, as Quixotic as it may sound, a well in every village.

Of more immediate purpose within the jurisdiction of the Committee, the assets and cash flow that we seek to freeze and disrupt are located abroad. International cooperation is therefore critical, and it requires a new mind set in intelligence that will inform both the nature and manner of collection. Our new secrets must be collected with the intention of sharing, and strong enough to withstand a measure of judicial scrutiny. That is a sea change required by the developing jurisprudence of terrorism and its focus on prevention, rather than punishment.

In addition, if Madrid has any lessons – terrorism funded through criminal activity – local law enforcement must be integrated more directly with the national intelligence community to facilitate a two way dialogue of increasingly equal value. Finally, we must vest an agency of the U.S. government with the power to direct and execute the campaign against terrorist financing. The NSC is not the appropriate place to direct a theater of war.

The man who straps a bomb to his chest as he enters a marketplace is an implacable foe. He is beyond redemption and cannot be deterred. It would be the height of irony – and perhaps the promise of future tragedy – if we permit the orthodoxy of how we have organized government, and collected and acted upon intelligence in the past to deter us from responding in the future.

Post-Hearing Questions for the Record
Submitted to Lee S. Wolosky
From Senator Daniel Akaka

"An Assessment of Current Efforts to Combat Terrorism Financing"

June 15, 2004

1. There have been reports in the media that the joint U.S.-Saudi task force has been working. However, it is my understanding that U.S. participants have only requested low level documents to avoid having further requests denied.

   In your expert opinion, how effective has the joint task force investigated terrorism financing?

   Answer: Because I am not privy to the work of the joint U.S.-Saudi task force, it is difficult to offer a confident assessment. However, it does not appear that the work of this task force – the formation of which was publicly announced almost a year ago – has lead to any terrorist financing-related arrests or prosecutions. I would encourage the committee to seek to confirm that fact and to ascertain whether the joint task force is achieving success by other metrics.

2. Appendix C of the Council's report states that "Saudi compliance with counter-terrorist financing measures is relatively strong."

   But, Appendix B – the Technical Assessment of Saudi Arabian Law – indicates that the Saudi government has failed to implement their new terrorism financing laws. This Appendix presents a devastating pattern of failure by the Saudis to confront terrorism financing.

   On a scale of A to F, what overall grade would you give the Saudis?

   Answer: Appendix C to the Task Force Report analyzes the Saudi response on a comparative basis, principally by analyzing the Saudi response to terrorist financing to that of other nations in the Muslim world. On this comparative basis, it gives the Saudi response relatively high marks. Appendix B to the Report and the Report itself do not use that comparative basis as a benchmark; they seek rather to analyze the Saudi response in relation to international best practices and the broad imperatives of U.S. national security, respectively. Here, there are certain deficiencies, as identified in the text. So on balance, it is difficult to offer a single, overall "grade" to the Saudi response. It depends on the relevant benchmarks.

Post-Hearing Questions for the Record
Submitted to Mallory Factor
From Senator Daniel Akaka

"An Assessment of Current Efforts to Combat Terrorism Financing"

June 15, 2004

1. Appendix C of the Council's report states that "Saudi compliance with counter-terrorist financing measures is relatively strong."

   But, Appendix B – the Technical Assessment of Saudi Arabian law – indicates that the Saudi government has failed to implement their new terrorism financing laws. This Appendix presents a devastating pattern of failure by the Saudis to confront terrorism financing.

   On a scale of A to F, what overall grade would you give the Saudis?

Answer: If Saudi Arabia is compared to other nations in the Islamic world, as Appendix C to the Task Force Report does, I believe that the Saudis have been relatively successful in putting into place a legal and regulatory framework designed to combat terror financing. Thus, on this comparative basis, the Saudis have earned a passing mark in this regard. In contrast, however, if the effectiveness of the Saudi new regime against terror financing is evaluated based on evidence we were able to obtain, I believe that the Saudis do not yet earn a passing grade in actually curbing terror financing. Such an evaluation is made in the core Task Force Report and Appendix B, and I believe that my assessment of Saudi Arabia on this subject is consistent with the Task Force as a whole.

Post-Hearing Questions for the Record
Submitted to the Honorable David D. Aufhauser
From Senator Daniel Akaka

"An Assessment of Current Efforts to Combat Terrorism Financing"

June 15, 2004

1. Saudi Arabia has yet to comply with the United States' request that the former head of Al Haramain, be arrested for his involvement in terrorist activities. Al-Aqil is on the United States' terrorist watch list and is believed to have sufficient resources and connections to continue supporting terrorist organizations.

   How much credibility can we put on Saudi Arabia's recent efforts when it continues to overlook his crimes?

   Should we take this as a sign of the government's lack of commitment to cracking down on those who finance terrorist activities?

Response:

As I have said before, much of the Saudi initiatives against terrorist financing have focused upon changing their system on regulation and oversight. Very little has resulted in holding people personally accountable. Failure to proceed against Al-Aqil is, perhaps, the most striking example of the continuing failure to address the issue of personal accountability. They will not succeed in fighting terrorism unless they hold the bankers of terrorism accountable.

2. Appendix C of the Council's report states that "Saudi compliance with counter-terrorist financing measures is relatively strong."

   But, Appendix B – the Technical Assessment of Saudi Arabian law – indicates that the Saudi government has failed to implement their new terrorism financing laws. This Appendix presents a devastating pattern of failure by the Saudis to confront terrorism financing.

   On a scale of A to F, what overall grade would you give the Saudis?

Response:

This question is really best addressed to the Council on Foreign Relations. My net assessment is that much of what has been done is form over substance and doesn't make any of us any safer

An Update on the Global Campaign Against Terrorist Financing

Second Report of an Independent Task Force on Terrorist Financing
Sponsored by the
Council on Foreign Relations

Maurice R. Greenberg,
Chair

Mallory Factor,
Vice Chair

William F. Wechsler and Lee S. Wolosky,
Project Co-Directors

June 15, 2004

The Council on Foreign Relations is dedicated to increasing America's understanding of the world and contributing ideas to U.S. foreign policy. The Council accomplishes this mainly by promoting constructive debates and discussions, clarifying world issues, and publishing *Foreign Affairs,* the leading journal on global issues. The Council is host to the widest possible range of views, but an advocate of none, though its research fellows and Independent Task Forces do take policy positions. Please visit our website at www.cfr.org.

The Council will sponsor an Independent Task Force when (1) an issue of current and critical importance to U.S. foreign policy arises, and (2) it seems that a group diverse in backgrounds and perspectives may, nonetheless, be able to reach a meaningful consensus on a policy through private and nonpartisan deliberations. Typically, a Task Force meets between two and five times over a brief period to ensure the relevance of its work.

Upon reaching a conclusion, a Task Force issues a report, and the Council publishes its text and posts it on the Council website. Task Force Reports can take three forms: (1) a strong and meaningful policy consensus, with Task Force members endorsing the general policy thrust and judgments reached by the group, though not necessarily every finding and recommendation; (2) a report stating the various policy positions, each as sharply and fairly as possible; or (3) a "Chair's Report," where Task Force members who agree with the Chair's Report may associate themselves with it, while those who disagree may submit dissenting statements. Upon reaching a conclusion, a Task Force may also ask individuals who were not members of the Task Force to associate themselves with the Task Force Report to enhance its impact. All Task Force Reports "benchmark" their findings against current administration policy in order to make explicit areas of agreement and disagreement. The Task Force is solely responsible for its report. The Council takes no institutional position.

For further information about the Council or this Task Force, please write to the Council on Foreign Relations, 58 East 68th Street, New York, NY 10021, or call the Director of Communications at (212) 434-9400. Visit our website at www.cfr.org.

CONTENTS

FOREWORD

Few aspects of the global war on terror are as inscrutable as the battle being waged on the financial front. Money for al-Qaeda and other terrorist groups is raised and moved worldwide and channeled through a web of institutions and individuals. The United States, other governments, the UN, and a range of international organizations have grappled with how best to address this daunting challenge.

My predecessor, Leslie H. Gelb, established the Independent Task Force on Terrorist Financing in 2002 to evaluate U.S. efforts to disrupt the financing of terrorist activities. The first report, chaired by Maurice R. Greenberg, concluded that although al-Qaeda's finances had been disrupted, they had not been destroyed—and that as long as al-Qaeda retained access to a viable financial network, it would remain a threat to the United States. The initial report recommended a series of steps to ensure a more effective U.S. and international response to al-Qaeda's global financial network.

Subsequent world events—including the May 2003 Riyadh bombings and the war in Iraq—made it clear that a further review of efforts of the U.S. and Saudi governments to curtail terrorist financing was warranted. In this update, the Task Force reports both on important achievements and on the work that remains to be done. The Task Force, composed of a bipartisan group of experts from the foreign policy, business, law enforcement, and intelligence communities, makes a series of recommendations to redouble efforts to frustrate al-Qaeda's financial network.

This Task Force would not have been possible without the leadership of Maurice R. Greenberg. I am grateful to Hank for continuing to spearhead this effort. I am also pleased that Mallory Factor has teamed up with Hank to serve as his vice chair. Thanks, also, to William F. Wechsler and Lee S. Wolosky, who continued to serve as co-directors of this update, which makes another important contribution to an issue of vital national and international importance.

Richard N. Haass
President
Council on Foreign Relations
June 2004

ACKNOWLEDGMENTS

This report is the result of the hard work and support of a number of dedicated individuals of both political parties who seek to further critical national interests. We are, once again, grateful for the hard work and dedication put forth by all Task Force members. Our members brought unique backgrounds and areas of expertise to this complicated issue, and all worked hard to reach consensus under a tight schedule.

Much of the information concerning the subject of terrorist financing is highly classified. The report of this Task Force, comprised entirely of former governmental officials and private citizens, is necessarily limited to the realm of the unclassified. Moreover, the response of foreign nations to the financing of terrorism is frequently exceptionally nuanced. Conclusions regarding the nature and adequacy of that response are necessarily shaped by the social and professional backgrounds of those drawing the conclusions. Not unrelatedly, while sometimes public pressure is indispensable in diplomacy, it can also be the case that pushing too hard and publicly on sensitive matters can risk entrenchment and less progress on important issues than can more cautious and discrete approaches. Nevertheless, with those caveats in mind, we hope that this report will help promote an informed debate and discussion in our open society on the public record concerning a subject that remains largely opaque.

We are particularly grateful to our chair, Maurice R. Greenberg, for his stewardship of this project and his broader leadership in assuring continued attention to, and scholarship on, issues at the intersection of global finance and national security. Sustained attention to these issues will be critical to the success of the U.S.-led war on terrorism. With the limited exception of work now being performed by the Watson Institute for International Studies at Brown University, they are, to the best of our knowledge, the subject of no other sustained, appropriately funded scholarship at U.S. universities, think tanks, or nongovernmental organizations.

We also wish to thank Mallory Factor, the Task Force's vice chair, for his dedication to these issues and his extraordinary efforts to advance the mission of the Task Force.

The Task Force's deliberations benefited considerably from input from senior members of the U.S. Treasury Department and the National Security Council, and from discussions with officials of the Central Intelligence Agency. We are extraordinarily grateful to the U.S. officials

who have assisted our work. We are also grateful to Adel al-Jubeir, foreign policy adviser to Saudi Crown Prince Abdullah, for his interest in our work.

We also benefited from the assistance of the Council's Lee Feinstein, Lindsay Workman, Jennifer A. Manuel, Margaret Winterkorn-Meikle, and Maria J. Kristensen, and we are grateful for all they did to make this Task Force a success. The resources and expertise of the Watson Institute were especially valuable, and we are grateful to the Institute's Thomas Biersteker and Sue Eckert for their major contributions to our Task Force mission.

We would also like to express our deep gratitude to the team from Columbia University's School of International and Public Affairs, Business School, and Law School that researched applicable Saudi Arabian laws and regulations for the Task Force, and whose assessment is referenced in this report: Nicholas Barnard, Seung Woo Chun, Mohamed Essakali, Yair Galil, Ilan Goldenberg, Reginald King, Duncan Long, Jennifer Mendel, Mihaela Nistor, Mitch Silber, Sean Smeland, Anuj Tiku, Deepak Venkatachalam, Michael Wallach, Ryan Wallerstein, and Suh-Kyung Yoon. They are an unusually talented group who brought enthusiasm, diligence, and strong analytical skills to this project. We are especially appreciative of the hard work done by the team leader, Mitch Silber, and for high-quality follow-up work undertaken by Yair Galil.

We would also like to extend special thanks to Christopher Blanchard and Martina Strazanova, rising stars in this new field, both of whom offered expert assistance and consistently wise counsel in the preparation of this report.

Finally, we wish to thank Council President Richard N. Haass for his continued support of our work and Council President Emeritus Les Gelb, whose initial vision made this Task Force a reality.

William F. Wechsler

Lee S. Wolosky

INTRODUCTION

In October 2002, this Task Force issued its initial report on terrorist financing. That report described the nature of the al-Qaeda financial network, the actions that had been taken to date to combat terrorist financing, and the obstacles that hindered those efforts.

Among our core findings was that, after a promising start in the immediate wake of 9/11, the U.S. government's efforts to combat terrorist financing remained "inadequate to assure sustained results commensurate with the ongoing threat posed to the national security of the United States." A key problem, we found, was that "deficiencies in political will abroad—along with resulting inadequacies in regulatory and enforcement measures—are likely to remain serious impediments to progress." Specifically, our initial report concluded:

> It is worth stating clearly and unambiguously what official U.S. government spokespersons have not: For years, individuals and charities based in Saudi Arabia have been the most important source of funds for al-Qaeda; and for years, Saudi officials have turned a blind eye to this problem.

Our Task Force report also included a number of specific strategic and tactical recommendations to help remedy these problems. Our core recommendations included two organizational ones. We recommended centralizing authority for policy formation and implementation on these issues within the White House. On the international front, we recommended the creation of a new multilateral organization to facilitate international cooperation.

We also recommended the encouragement of the Saudi regime to strengthen significantly its efforts to combat terrorist financing. In this regard, we noted a recent historical record of inattention, denial, and half measures.

We recommended directly confronting the lack of political will in Saudi Arabia and elsewhere through the institution of a declaratory policy that would permit or compel U.S. officials to speak more frankly about the nature of the problem:

> Put issues regarding terrorist financing front and center in every bilateral diplomatic discussion with every 'front-line' state in the fight against terrorism—at every level of the bilateral relationship, including the

> highest. Where sufficient progress is not forthcoming, speak out bluntly, forcefully, and openly about the specific shortfalls in other countries' efforts to combat terrorist financing. The Task Force appreciates the necessary delicacies of diplomacy and notes that previous administrations also used phrases that obfuscated more than they illuminated when making public statements on this subject. Nevertheless, when U.S. spokespersons are only willing to say that 'Saudi Arabia is being cooperative' when they know very well all the ways in which it is not, both our allies and adversaries can be forgiven for believing that the United States does not place a high priority on this issue.

The reaction to the release of the Task Force's initial report was reflective of then-prevailing mindsets. The Saudi Arabian Foreign Minister, Prince Saud al-Faisal, told CNN that the report was "long on accusation and short on documented proof." The Saudi ambassador to the United States, Prince Bandar bin Sultan, said the Task Force report was based on "false and inconclusive information" and "clearly out of touch with current activities." He also maintained that "Saudi Arabia has put into place the tools, resources, laws, and regulations to combat terrorism and terrorist financing" and promised to "prosecute the guilty to the fullest extent of the law." The U.S. Treasury Department's spokesperson called the report "seriously flawed."[1]

Meanwhile, the executive branch continued to grapple throughout the fall of 2002 and thereafter with how best to address the problem of Saudi individuals and organizations that it believed to be financing al-Qaeda and other terrorist organizations. In November 2002, a National Security Council Task Force was reportedly prepared to recommend to President George W. Bush an action plan designed to force Saudi Arabia to crack down on terrorist financiers within ninety days or face unilateral U.S. action. During 2002 and into the first few months of 2003, U.S. officials engaged their Saudi counterparts on a sustained basis in Washington and Riyadh—at increasingly high levels, with more intelligence they were prepared to share, and with more aggressive demands.

---

[1] Elsewhere, the reaction to the report was more positive. Members of Congress, for example, broadly endorsed the report and sought to implement certain of its recommendations. On July 30, 2003, a bipartisan group of 111 members of the House of Representatives led by Rep. Jim Davis (D-FL) and including the chair of the International Relations Committee, chair of the Financial Services Committee, chair of the Appropriations Committee, and the vice chair of the Intelligence Committee, wrote to the president to ask that he accept a key recommendation of the Task Force and centralize authority for this issue in the White House. Earlier, on July 16, Rep. Nita Lowey (D-NY) led efforts to increase funding for the Treasury's Office of Technical Assistance, citing a recommendation of our initial report. On November 18, 2003, Senator Arlen Specter (R-PA) cited the findings of our report when introducing the Saudi Arabia Accountability Act of 2003, a bill that would impose certain sanctions on Saudi Arabia unless the president certifies that it is cooperating with U.S. efforts to combat terrorism.

Less transparent methods of curtailing terrorist financing were also stepped up, with significant successes. Although these activities are clearly relevant to the subject matter of this report, for obvious reasons they cannot be addressed in a report such as this one, which must necessarily cite only public information and public statements.

Perhaps out of concern that more direct public statements would have negatively affected increasingly aggressive private demands, the U.S. executive branch's public statements regarding terrorist financing largely remained unchanged. In public, White House and State Department spokespersons continued to refuse to criticize the job Saudi Arabia was doing to combat terrorist financing; indeed, the same week of public reports concerning the possible imposition by the president of unilateral sanctions, the White House spokesperson maintained that Saudi Arabia was a "good partner in the war on terrorism." For their part, Saudi officials continued to maintain that they were taking all necessary and possible steps to combat terrorism and terrorist financing.

The status quo changed on May 12, 2003, when al-Qaeda bombed housing compounds in Riyadh used by U.S. and other foreign residents, prompting more comprehensive Saudi action against terrorism. The need for this action was demonstrated again on November 9, 2003, when a similar al-Qaeda–directed attack took place at another Riyadh housing compound, and on April 21, 2004, when another attack took place in Riyadh, this time against the General Security building. Most recently, at the beginning and end of May 2004, two attacks targeted the Saudi oil industry. They took place in Yanbu and Khobar, respectively, with the latter attack and hostage-taking resulting in twenty-two fatalities.[2]

---

[2] The strategic decision to launch attacks within Saudi Arabia was apparently controversial within the al-Qaeda movement, in part because of the possible negative impact on fundraising within the Kingdom. The second issue of "The Voice of Jihad," a biweekly online magazine identified with al-Qaeda, contains an October 2003 interview with Abd Al-'Aziz bin 'Issa bin Abd Al-Mohsen, also known as Abu Hajjer, an al-Qaeda member ranking high on Saudi Arabia's most-wanted list. Abu Hajjer remarked: "Jihad members and lovers of Mujahideen were split: There were those who said we must attack the invading forces that defile the land of the two holy places, and that we must turn the Americans' concerns to themselves and their bases, so they would not take off from there to crush Muslim lands and countries, one by one. There were others who said we had to preserve the security of this base and this country [i.e., Saudi Arabia], from which we recruit the armies, from which we take the youth, from which we get the [financial] backing. It must therefore remain safe. My opinion is midway between the two... It is also true that we must use this country [Saudi Arabia] because it is the primary source of funds for most Jihad movements, and it has some degree of security and freedom of movement. However, we must strike a balance between this and the American invasion of the Islamic world and its [strangling of] the Jihad movement and even other Islamic movements. ..."

Public statements and actions by both the United States and Saudi Arabia since May 2003 have evidenced in many respects a more urgent approach to terrorist financing, one that is broadly consistent with our initial report's conclusions, findings, and recommendations. For example, Saudi Arabia has announced a profusion of new laws, regulations, and institutions regarding money laundering, charitable oversight, and the supervision of the formal and informal financial services sector. Significantly, the government also took steps to remove donation boxes from mosques and shopping malls. And, for the first time, Saudi Arabia has subjected its anti–money laundering regime to international scrutiny. Recently, the Financial Action Task Force (FATF)—a thirty-three–member international body dedicated to promulgating international anti–money laundering and counterterrorist financing (AML/CTF) standards—conducted an in-depth review of Saudi Arabia's overall AML/CTF regime. FATF is in the process of completing its assessment and is expected to issue a "summary report" shortly. Early indications suggest that the new Saudi laws and regulations meet or exceed international standards in many respects and will receive a passing grade.

While Saudi officials were previously unwilling to acknowledge or address the role government-sanctioned religious messages play in supporting militant Islamic groups, following the May terrorist attacks Saudi officials began to take steps to address the mindset that foments and justifies acts of terrorism. This has included educational reform and steps intended to discipline (or "re-educate") certain extremist Islamic clerics—at least those operating in Saudi Arabia. Several such clerics have publicly dissociated themselves from extremism on state-controlled television.

Most critically, for the first time, the Saudi government decided to use force to hunt—and kill—members of domestic al-Qaeda cells, including, in one case, a financier named Yousif Salih Fahad Al-Ayeeri (aka "Swift Sword"). Actions on this scale were not in evidence prior to the 2003 bombings.

The Bush administration acted quickly to take advantage of newfound political will in Saudi Arabia to renew and reinvigorate its own efforts to combat terrorist financing. In August 2003, the United States and Saudi Arabia announced the creation of the Joint Terrorist Financing Task Force, based in Riyadh. Through this Task Force, investigators from the FBI and from the Internal Revenue Service Criminal Investigation Division (IRS-CID) have developed "agent-to-

agent" working relationships with their Saudi counterparts and, for the first time, have gained direct access to Saudi accounts, witnesses, and other evidence.

The pace of joint U.S.-Saudi designations quickened, specifically in respect to efforts to close problematic overseas branches of the sprawling, Saudi-based Al Haramain Islamic Foundation, which Saudi officials estimate was, at its height, raising between forty and fifty million dollars per year. On December 22, 2003, for example, the United States and Saudi Arabia jointly designated Vazir—a nongovernmental organization located in Travnik, Bosnia—after it was determined that it was the reincarnation of the previously designated Al Haramain-Bosnia. Bosnian authorities then raided and closed this organization. The two governments also designated Safet Durguti, the representative of Vazir. On January 22, 2004, the United States and Saudi Arabia announced a joint decision to refer four additional branches of Al Haramain to the UN's al-Qaeda and Taliban Sanctions Committee (the 1267 Committee). These branches—located in Indonesia, Kenya, Tanzania, and Pakistan—had, according to the two governments, provided financial, material, and logistical support to the al-Qaeda network and other terrorist organizations.

The United States and Saudi Arabia announced on June 2, 2004 the designation of five additional branches of Al Haramain located in Afghanistan, Albania, Bangladesh, Ethiopia, and the Netherlands. The United States also announced the designation of Al Haramain's founder and former leader, Aqil Abdulaziz Al-Aqil.

Even more significantly, the government of Saudi Arabia announced the dissolution of Al Haramain and other charitable entities and the creation of a nongovernmental organization to coordinate private Saudi charitable giving abroad.

As a result of the foregoing activities, al-Qaeda's current and prospective ability to raise and move funds with impunity has been significantly diminished. These efforts have likely made a real impact on al-Qaeda's financial picture, and it is undoubtedly a weaker organization as a result. Much of the impact has been through deterrence—i.e., past or prospective donors are now less willing to support organizations that might be complicit in terrorism.

Key agencies in our government have also grown more accustomed to working with one another in new ways and become better at accommodating one another's interests. The CIA and the FBI, in particular, cooperate closely up and down the chain of command, on both a tactical and strategic level.

The record is more mixed when it comes to the implementation of our recommendation that U.S. officials speak clearly, openly, and unambiguously about the problems of terrorist financing. Official reports, such as the State Department's latest Patterns of Global Terrorism report, continue to give praise where praise is due but too often go to lengths to avoid explicit statements about the steps yet to be taken.[3] However, there have been important exceptions to this rule.

On June 26, 2003, for example, at the annual U.S.-EU Summit, President Bush took the important step of publicly urging European leaders to criminalize all fundraising by Hamas, another recommendation of our Task Force report. Extensive work by the State and Treasury Departments preceded and followed up the president's strong remarks. On September 6, 2003, despite longstanding European insistence that Hamas's "political wing" is distinct from its "military wing," the European Union officially added Hamas to its list of banned terrorist groups.

Even more significantly, the same day that President Bush met with his European counterparts, David Aufhauser, the then-general counsel of the Treasury and chairman of the National Security Council's Policy Coordination Committee on Terrorist Financing, testified before Congress that "in many ways, [Saudi Arabia] is the epicenter" of the financing of al-Qaeda and other terrorist movements. This statement of fact—clear to U.S. officials of two administrations since the late 1990s—mirrored a core conclusion of our initial report. It also reflected an implementation of our core recommendation that senior U.S. officials move toward a more frank declaratory policy on these issues.

At the same time, during the summer of 2003, the Treasury Department declined to provide to Congress a list of Saudi persons and individuals recommended for unilateral enforcement action,[4] and the Bush administration declined to declassify twenty-eight pages of a

[3] Among other things, *Patterns* states: "Saudi Arabia has launched an aggressive, comprehensive, and unprecedented campaign to hunt down terrorists, uncover their plots, and cut off their sources of funding" and "Riyadh has aggressively attacked al-Qaida's operational and support network in Saudi Arabia and detained or killed a number of prominent operatives and financial facilitators... Senior Saudi government and religious officials espouse a consistent message of moderation and tolerance, explaining that Islam and terrorism are incompatible." While we largely concur with these statements, we also believe that official statements and reports should set forth with particularity shortcomings as well as praise, to serve as a benchmark for future progress. For these and other reasons, we have recommended not only a more declaratory U.S. policy but also the imposition of a comprehensive certification regime that would include detailed findings of fact, as set forth on pages 31 and 32 *infra*.

[4] Relevant committees of the Congress were provided with a classified listing of the number of Saudi entities and individuals considered for designation, as well as a number of classified briefings regarding this issue.

joint congressional report that reportedly detailed the role of Saudi persons or organizations in the 9/11 attacks.

At the end of 2003, two reports concluded that U.S. efforts to combat terrorist financing had yet to accomplish the basic mission of stopping the flow of money to terror groups. The U.S. General Accounting Office, the investigative arm of Congress, concluded that federal authorities still did not have a clear understanding of how terrorists move their financial assets and continue to struggle to halt terrorist funding. The United Nations Monitoring Group, in its second required report to the UN's al-Qaeda and Taliban Sanctions Committee, also found that "al-Qaeda continues to receive funds it needs from charities, deep-pocket donors, and business and criminal activities, including the drug trade. Extensive use is still being made of alternative remittance systems, and al-Qaeda has shifted much of its financial activity to areas in Africa, the Middle East and South-East Asia where the authorities lack the resources or the resolve to closely regulate such activity."

The views expressed in the Task Force's first report are now widely held, at home and abroad. Combating terrorist financing must remain a central and integrated element of the broader war on terrorism, and Saudi Arabia should be—and is—taking important efforts in this regard. Effective international efforts will continue to require both strong U.S. leadership and sustained political will in the source and transit countries for the funds that continue to support international terrorist organizations such as al-Qaeda. As a senior Treasury Department official told Congress on March 24, 2004, "we have found that our success is also dependent on the political will and resources of other governments."

It is with these thoughts in mind that we offer the findings and recommendations that follow. We note at the outset that much of the discussion in the text of this report and in the appendixes concerns Saudi Arabia. That is certainly not because we believe that Saudi Arabia is alone in the need to take effective and sustained action to combat terrorist financing. Indeed, on a comparative basis Saudi Arabia has recently taken more decisive legal and regulatory action to combat terrorist financing than many other Muslim states. Nor is it to minimize the potential significance of new modalities of terrorist financing that have nothing to do with individuals and organizations based in Saudi Arabia. Al-Qaeda financing has almost certainly become more diffuse since the dispersal of its leadership from Afghanistan; whereas once al-Qaeda's funds were managed centrally, communication and logistical difficulties have forced local operatives in

many cases to improvise and fend for themselves.[5] Rather, it is because of the fundamental centrality that persons and organizations based in Saudi Arabia have had in financing militant Islamist groups on a global basis—a fact that officials of the U.S. government have now joined this Task Force in publicly affirming.

[5] The Madrid bombing investigation, for example, indicates that the cell responsible for the March 2004 train bombing in that city relied significantly on self-help and drug trafficking to fund its operations.

FINDINGS

As a general matter, we wish to reaffirm the principal "findings" of our initial report, reproduced here in Appendix A. Although progress has been made on several important fronts, al-Qaeda and other terrorist organizations, as demonstrated by recent attacks and related investigations, still have ready access to financial resources, and that fact constitutes an ongoing threat to the United States (among other states). The problem has not been solved and, as we noted in our initial report, there is no single "silver bullet" to end the financing of terror. With those thoughts in mind, we wish to make the following additional findings regarding the state of efforts to combat terrorist financing since the issuance of our last report.

1. *Various international fora are engaged in a wide array of multilateral activities that collectively constitute a new international regime for combating terrorist financing.* In our initial report, we recommended the creation of a new international organization dedicated solely to issues involving terrorist financing. We find that many of the activities we envisioned such an organization undertaking are now underway under the leadership of existing international institutions and regimes, mitigating the need for a new specialized international organization. Specifically, we note that:
   - In September 2001, only four countries had ratified the International Convention for the Suppression of the Financing of Terrorism; by the end of April 2004, that number had increased to 117 states.
   - The United Nations Counter-Terrorism Committee (CTC), established by Security Council Resolution 1373, requires all member states to criminalize the provision of financial support to terrorists and to freeze terrorist assets. Significant progress has been achieved in focusing states' attention on implementation measures—all 191 countries have submitted first-round reports to the CTC, and many are engaged in the CTC's initiative to enhance compliance. The greatest impact of the UN's efforts has been in the adoption of national terrorist financing legislation, formation of domestic institutions such as Financial Intelligence Units (FIUs), and the identification of technical assistance needs of states. While the CTC's momentum slowed in late 2003, the Security Council, with strong U.S. support, adopted new measures in March to

"revitalize" the CTC as the primary mechanism to assist states in combating terrorist financing.

- The G8 established a Counter-Terrorism Action Group (CTAG) at the Evian Summit in June 2003 to assist the CTC in coordinating capacity-building assistance. The CTAG represents a potentially significant effort by donor nations to supplement the UN's capacity-building initiatives.
- The Financial Action Task Force (FATF) has played an important role in responding to 9/11 by promulgating its Eight Special Recommendations Against Terrorist Financing, establishing a methodology for assessing compliance with the eight recommendations, and issuing guidance for financial institutions in detecting terrorist financing, as well as developing best practices concerning the freezing of terrorist assets, alternative remittances, and nonprofit organizations. The FATF is also refocusing its efforts to ensure more effective implementation. The recent renewal of the FATF mandate shows the commitment of states to these issues.
- The UN's al-Qaeda and Taliban Sanctions Committee has expanded the list of terrorist entities against which all states are required to restrict financing. The Sanctions Committee has steadily improved the amount of detailed identifying information on listed individuals and increased its oversight and monitoring of states' implementation and enforcement efforts.
- Since the publication of our initial report, FATF has also reviewed Saudi Arabia's laws and regulations, an action it had previously not taken.
- In collaboration with the FATF, the International Monetary Fund (IMF) and World Bank have assessed forty-one countries' compliance with anti–money laundering and countering terrorist financing (AML/CTF) standards in a pilot program. Results indicate that while many jurisdictions are doing a good job countering money laundering, some were lagging behind in measures to deter terrorist financing. In April 2004, the IMF and World Bank agreed to continue the assessments as part of the ongoing Financial Sector Assessment Program (FSAP) and Reports on the Observance of Standards and Codes (ROSCs) but to adopt a more comprehensive and integrated approach to conducting assessments.

- Cooperation on terrorist financing has become a permanent part of the agendas of regional organizations such as the EU, Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), the Gulf Cooperation Council (GCC), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), and the African Union, as recommended by our first report. In the aftermath of the March 11 terrorist attacks in Madrid, the EU adopted a Terrorism Action Plan, including new proposals to strengthen the fight against terrorist financing through enhanced customs controls on cash movements, establishment of an electronic database of all targeted persons and entities, and possible modification of the procedures requiring unanimity for revisions of the list of terrorist organizations and assets. APEC established a Counter-Terrorism Action Plan, with a specific checklist of measures and a timeframe for members to halt the financing of terrorism.
- As countries reach a clearer understanding of what is required to stem terrorist financing, the number of requests for training and capacity-building technical assistance have increased. By the end of 2003, more than 160 states had requested or received capacity-building assistance from the CTC. The World Bank reported receiving more than 100 requests from countries to help build capacity to fight money laundering and terrorist financing. The CTC has facilitated assistance in drafting anti–terrorist financing legislation, support to banking supervisory bodies, and establishment of FIUs in almost sixty cases, with eighty-nine countries participating in workshops; countering terrorist financing training has been provided to seventy-one countries thus far.

2. *Saudi Arabia has taken important actions to disrupt domestic al-Qaeda cells and has improved and increased tactical law enforcement and intelligence cooperation with the United States, though important questions of political will remain.* Saudi actions to disrupt, degrade, and destroy domestic al-Qaeda cells are an extremely welcome development since the issuance of our last report. Interior Ministry and other Saudi law enforcement and intelligence officials are now regularly killing al-Qaeda members and sympathizers in violent confrontations—and are just as regularly being killed by them on the streets of Saudi Arabia.

As previously noted, the Task Force recognizes that non-public activities may affect an assessment of the terrorist financing issue, including in the context of the U.S.-Saudi relationship. There may be actions being taken by Saudi officials that are not being made public, some of which may involve cooperation with the United States. There may also be U.S. operations undertaken on the Arabian peninsula or elsewhere that implicate Saudi national interests but that are taking place without Saudi knowledge. All of these possibilities may affect the subject matter of this report. But none is a matter of public knowledge, and these possibilities, accordingly, cannot be addressed in this report. We find that operational law enforcement and intelligence cooperation on counterterrorism matters have markedly improved since the issuance of our last report.

We note that while Saudi actions following May 2003 in confronting al-Qaeda within the Kingdom evidenced vastly increased political will, anomalous elements remained. For example, following the May 2004 attack in Yanbu, Saudi Crown Prince Abdullah said in remarks broadcast on Saudi TV that "Zionism is behind terrorist actions in the Kingdom... I am 95 percent sure of that." Several days later Saudi Foreign Minister Prince Saud Al-Faisal reaffirmed the crown prince's remarks, noting, "It is not hidden from anyone that extremist Zionist elements are engaging in a vulgar campaign against the kingdom by espousing and disseminating lies and incitement against the Saudi government.... The terror operations taking place today serve the interests of the extremist Zionist elements, and this means that they [the perpetrators of the operations and the Zionist elements] share common interests." Saudi Interior Minister Prince Nayef bin Abdul Aziz, asked whether there was a contradiction between these statements and his own statements attributing attacks in the Kingdom to al-Qaeda, reportedly said, "I don't see any contradiction in the two statements, because al-Qaeda is backed by Israel and Zionism."

To the best of our knowledge, these statements were never retracted; indeed, at a press conference in Washington on June 2, 2004, neither Adel al Jubeir, the foreign policy adviser to the crown prince, nor a State Department official by his side repudiated them in specific response to questions from reporters. These statements compromise the moral clarity of Saudi actions and the overall effort to change the mindset that foments extremism.

We also note that few al-Qaeda operatives are being captured alive, which also means that few are made available for questioning by foreign law enforcement or intelligence agencies. And, to date, financiers have largely remained beyond the scope of the more forceful and transparent domestic Saudi enforcement efforts, as described below more fully.

3. *Saudi Arabia has made significant improvements in its legal and regulatory regime.* We noted in our initial report that "In 1999... Saudi Arabia approved amendments to its existing money laundering laws intended to bring it into compliance with international standards, but to date these amendments have not been implemented, according to the most recent State Department reports." Since the issuance of our initial report—and particularly since the May 2003 Riyadh bombings—Saudi Arabia has announced the enactment or promulgation of a profusion of new laws and regulations and the creation of new institutional arrangements, that are intended to tighten controls over the principal modalities of terrorist financing. Given the historical centrality of funds from Saudi-based individuals and organizations to the problem of terrorist financing, the Task Force considers these matters to be of fundamental relevance to the national security of the United States. Accordingly, since no public assessment of them was available, we commissioned a review of the new Saudi Arabian legal, regulatory, and institutional regime to combat money laundering and terrorist financing.[6] Excerpts of this comprehensive review, undertaken by graduate students from Columbia University's School of International and Public Affairs, Law School, and Business School, are cited and available on the Council's website at www.cfr.org.

   Regrettably, our efforts in this regard were hampered by the unwillingness of Saudi officials to provide a large amount of requested information. Despite a cordial and

[6] We commissioned this assessment with the knowledge that the FATF was likely to conduct a similar analysis. Indeed, we shared impressions with leaders of the FATF assessment during the pendency of the respective reviews, and we reached similar conclusions. We proceeded with an independent assessment notwithstanding the complementary FATF review because FATF reviews are not normally made entirely public and because the intergovernmental FATF operates by consensus, meaning that, as a general matter, U.S. concerns and perspectives may not ultimately be prioritized or articulated. Moreover, the FATF employs a generic methodology, meaning that country-specific issues, such as charities, may not receive attention that is commensurate with their importance from the standpoint of the country reviewed or from the standpoint of U.S. interests. And perhaps most significantly, while FATF assesses laws and regulations as they exist on paper, it does not normally assess *implementation and enforcement* of those laws and regulations, as discussed elsewhere in this report.

productive meeting with a senior Saudi official in June 2003, and notwithstanding the promise of full cooperation from the Kingdom of Saudi Arabia, we received only very limited cooperation.

Nevertheless, on the basis of our review of certain publicly available materials and our discussions with Saudi and U.S. officials, we find that Saudi Arabia has made significant improvements to its anti–money laundering and counterterrorist financing regime and has taken the following steps, among others, many of which are discussed and analyzed in greater detail in the above-mentioned review:

- Enactment last year of the new anti–money laundering law of 2003 and the issuance of anti–money laundering implementation rules earlier this year. Specific measures include, among other things, more comprehensive criminalization, improved reporting and record-keeping requirements applicable to the formal financial sector, new inter-agency coordination mechanisms, and the establishment of an FIU.[7]

- The imposition of mandatory licensing requirements and additional legal, economic, and supervisory measures for alternative remittance systems, such as *hawala*.

- New training programs for judges and law enforcement officials on anti–money laundering and counterterrorist financing.

- The announced freezing of assets of persons and organizations supporting terrorism.

- The promulgation last year of comprehensive new restrictions on the financial activities of Saudi-based charitable activities, along with additional oversight initiatives. As we described in our initial report and has been extensively reported elsewhere, Saudi-based charities have fueled radical Islamist activities in many parts of the world, including Asia, Africa, Europe, the Middle East, and North America. In some respects, the new restrictions that have been announced go further than those of any other country in the world, and include the following:

[7] See, generally, Royal Embassy of the Kingdom of Saudi Arabia, "Initiatives and actions taken by the Kingdom of Saudi Arabia in the war on terrorism," September 2003 (the "Green Book"). Available online at: http://www.saudiembassy.net/2003News/News/TerDetail.asp?cIndex=142.

- Provisions that limit or prohibit transfers from charitable accounts outside of Saudi Arabia.
- Enhanced customer identification requirements applicable to charitable accounts.
- Provisions requiring that charitable accounts be opened in Saudi Riyals.
- The announcement of the formation of a governmental High Commission of Oversight of Charities to oversee Saudi-based charities.
- The consolidation of charitable banking activities in one principal account. Although sub-accounts are permitted for branches, they are restricted to receiving deposits, and withdrawals and transfers must be serviced through the main account.
- The prohibition of cash disbursements from charitable accounts, along with the issuance of ATM or credit cards against such accounts.
- The banishment of unregulated cash contributions in local mosques and the removal of cash collection boxes for charities from shopping malls.
- The announced completion, on May 16, 2003, of audits of all Saudi-based charities.
- The announcement of the creation of the Saudi National Entity for Charitable Work Abroad, a nongovernmental body that, according to Saudi officials, is intended to assume all private overseas aid operations and responsibility for the distribution of private charitable donations from Saudi Arabia and into which other Saudi-based charities and committees operating internationally will be dissolved.

4. *Saudi Arabia has not fully implemented its new laws and regulations, and because of that, opportunities for the witting or unwitting financing of terrorism persist.* The passage of laws and regulations is only the first step toward the creation of an effective AML/CTF regime. Just as important—and more important over the longer term—is effective implementation. Some aspects of implementation—comprehensive and well-

informed compliance with record-keeping and auditing rules or fully staffing new organizations, for instance—may take time. However, many other aspects of implementation, such as standing up and funding new organizations and oversight bodies—can be accomplished more readily. Despite statements to the contrary, Saudi Arabian authorities did not fully cooperate with our requests for information on the status of their implementation of important aspects of their AML/CTF regime. Nevertheless, on the basis of information publicly available, we are able to conclude with confidence that official Saudi assertions, such as the June 12, 2003, Saudi embassy press release that claimed the Kingdom had "closed the door on terrorist financing and money laundering," remain premature.[8]

Since the issuance of our first report, the U.S. government has at times agreed with this assessment. On August 12, 2003, for example, Deputy Secretary of State Richard Armitage stated, "We found laws being changed and scrutiny directed towards the private charitable organizations to be greatly heightened. It is still not sufficient." More recently, on March 24, 2004, Juan Zarate, the senior Treasury Department official with responsibility for these issues, told Congress that the implementation of many of these measures by the Kingdom posed "ongoing challenges" and that a particularly "critical challenge... is fully implementing and enforcing the comprehensive measures [Saudi Arabia] has enacted to ensure charities are not abused for terrorist purposes."

Among other things, sustained attention to implementation is required in respect of legal, regulatory, and institutional reforms intended to impact the formal and informal financial sectors and the charities sector. Indicia of implementation and enforcement are generally unavailable. We are concerned that the unavailability of such indicia may negatively impact the deterrent effect presumably intended by these measures. As this report was going to press, for example, we were unable to find evidence to suggest that the announced High Commission of Oversight of Charities was fully operational. Moreover, its composition, authority, mandate, and charter remain unclear, as do important metrics of its likely effectiveness, such as staffing levels, budget, and personnel

[8] As part of the government of Saudi Arabia's offer of assistance to the work of our Task Force, we sought to visit Riyadh to discuss, among other things, the state and level of the implementation of these new laws, regulations, and oversight mechanisms. Despite a formal invitation from a representative of the crown prince, no visit was ever confirmed and scheduled by Saudi officials.

training. The mandate and authority of the High Commission of Oversight of Charities is also unclear relative to that of the Saudi National Entity for Charitable Work Abroad, which was first announced in February 2004.[9] As Juan Zarate told Congress earlier this spring, "the Kingdom must move forward to clarify and empower an oversight authority that will administer effective control over the [charity] sector and ensure compliance with obligations under the new regulatory measures." More recently, on June 2, 2004, Zarate called the establishment of the Saudi National Entity for Charitable Work Abroad a "major step forward" and noted, "we're looking forward to seeing the implementation of that."

At least one other key body, Saudi Arabia's FIU, is also not yet fully functional. FIU's are intended to collect and analyze suspicious financial data. Reliable, accessible metrics are lacking with respect to many of the other newly announced legal, regulatory, and institutional reforms. Critical data necessary to assess the implementation, enforcement, and effectiveness of many of these announced reforms are generally nonexistent or not publicly available. We find this troubling given the importance of these issues to the national security interests of the United States and other countries (including Saudi Arabia) that remain targets of al-Qaeda and similar terrorist organizations. The universal application of rule of law to prominent persons in Saudi Arabia, especially those close to members of the Saudi royal family, also remains uncertain.

5. *We have found no evidence that Saudi Arabia has taken public punitive actions against any individual for financing terror. As a result, Saudi Arabia has yet to demand personal accountability in its efforts to combat terrorist financing and, more broadly and fundamentally, to delegitimize these activities.* The lack of transparent and compelling

[9] The following statement was issued by the Royal Court on February 28, 2004: "In response to the merciful Shari'ah teachings which call for the brotherhood of the faithful, to enable the noble Saudi people to continue helping their Muslim brothers everywhere and to rid Saudi charity work abroad from any misdeeds that might undermine it or distort its reputation, the Saudi government has decided to put clear methodical rules to organize Saudi charity work abroad. In this context, the Custodian of the Two Holy Mosques King Fahd Bin-Abd-al-Aziz has issued order number A/1 dated on 6/1/1425 H. To approve the creation of a charity commission called "the Saudi Non-Governmental Commission for Relief and Charity Work Abroad." The state-controlled SPA news agency stated: "The royal order stated that the task of forming and administering the commission will be carried out by a selected group of citizens working in the charity field and enjoying experience, integrity and good reputation. The royal order also charged the commission exclusively with all charity work and relief abroad. The commission will announce its regulation and how it will work as soon as its creation is completed during the next few weeks."

evidence of implementation is particularly troublesome in the criminal law enforcement context. Despite the flurry of laws and regulations, we are aware of no publicly announced arrests, trials, or incarcerations in Saudi Arabia in response to the financing of terrorism—despite the fact that such arrests and other punitive steps have reportedly taken place. Against its poor historical enforcement record, any Saudi actions against financiers of terror are welcome. But actions taken in the shadows may have little consistent or systemic impact on ingrained social or cultural practices that directly or indirectly threaten the security of the United States.

Individuals and organizations based in Saudi Arabia long have been the most significant source of funds for al-Qaeda. As a general matter, such individuals and organizations have had close ties to the Saudi establishment. For example, Saudi government officials and members of the *ulema*, or clerical establishment, participate directly in the governance of Saudi charities.

Aggressive action against financiers therefore requires greater political will, not just action against the politically powerless or socially marginalized. So far, demonstrable evidence of this political will has been lacking. These concerns are even codified to a certain extent in Saudi Arabia's new anti–money laundering law, which appears to contain overly broad exemptions for "politically exposed persons" who might otherwise be subject to enhanced due diligence and reporting requirements.

Deeply ingrained social, cultural, and religious norms have facilitated and reinforced Saudi Arabia's status as the main source of financial support to groups such as al-Qaeda. Those norms must be fundamentally delegitimized. The public condemnation of extremism by senior Saudi officials, discussed in greater detail below, is an important start. But criminalization and public enforcement are also critical components of the delegitimization process. Without them, it is difficult to create deterrence and a governance system that demands personal accountability.

Put more simply: People and organizations need to be publicly punished, including for past involvement in terrorist financing activities.

Not only have there been no publicly announced arrests in Saudi Arabia related to terrorist financing, but key financiers remain free or go unpunished. For example, Yasin

al-Qadi, a Specially Designated Global Terrorist, appears to live freely in Saudi Arabia. According to the Treasury Department, "He heads the Saudi-based Muwafaq Foundation. Muwafaq is an al-Qaeda front that receives funding from wealthy Saudi businessmen. Blessed Relief is the English translation. Saudi businessmen have been transferring millions of dollars to bin Laden through Blessed Relief." Wa'el Julaidan, who was jointly designated on September 6, 2002, by the governments of the United States and Saudi Arabia as "an associate of Usama bin Laden and a supporter of al-Qa'ida terror," also appears to live freely in Saudi Arabia. According to the Treasury Department, "The United States has credible information that Wa'el Hamza Julaidan is an associate of Usama bin Laden and several of bin Laden's close lieutenants. Julaidan has directed organizations that have provided financial and logistical support to al-Qa'ida."[10] The same is true for Aqeel Abdulaziz Al-Aqil, the founder and long-time leader of the Al Haramain Islamic Foundation (AHF). According to the Treasury Department, "As AHF's founder and leader, Al-Aqil controlled AHF and was responsible for all AHF activities, including its support for terrorism.... Under Al Aqil's leadership of AHF, numerous AHF field offices and representatives operating throughout Africa, Asia, Europe and North America appeared to be providing financial and material support to the al-Qa'ida network. Terrorist organizations designated by the U.S. including Jemmah Islammiya, Al-Ittihad Al-Islamiya, Egyptian Islamic Jihad, HAMAS, and Lashkar E-Taibah received funding from AHF and used AHF as a front for fundraising and operational activities."

Since the issuance of our last report, knowledgeable U.S. officials have privately expressed frustration at Saudi Arabia's failure to act against, among others, specific and identified members of that country's merchant class. They have expressed concerns about Saudi Arabia's failure to punish, in a demonstrable manner, specific and identified leaders of charities found to be funneling money to militant Islamist organizations. Moreover, despite a promising start, the U.S.-Saudi Joint Terrorist Financing Task Force, as of June 2004, has generated no public arrests or prosecutions to our knowledge.

[10] Although the designation was jointly reported to the United Nations, Prince Nayef bin Abdul Aziz, the Saudi interior minister, publicly disavowed his government's designation of Julaidan within twenty-four hours after it was announced in the United States. On September 7, he reportedly stated: "Those who say this [about Julaidan] should provide the evidence they have to convince us. We do not accept that a Saudi citizen did any action against his religion and country, but we depend on facts."

These same U.S. officials have underscored the extent to which enforcement matters can be highly nuanced. Indeed, we recognize that our views regarding enforcement and deterrence are shaped by the nature of the open society in which we live. Saudi society is far more opaque. Measures that may have been taken within Saudi Arabia against financiers but that are not fully transparent to outside observers may certainly be meaningful within Saudi society. These nuances should inform the vigorous public debate on this matter. Although we have little context for judging these measures, we do question how effective non-public actions can ever be in changing social norms and achieving broad deterrence.

Moreover, notwithstanding the foregoing nuances, we find that a key barometer for measuring Saudi Arabia's commitment to combat terror financing is whether authorities there hold responsible senior members of the Saudi elite who conduct such activity. We find it regrettable and unacceptable that *since September 11, 2001, we know of not a single Saudi donor of funds to terrorist groups who has been publicly punished*—despite Ambassador Bandar's assertion, in response to the issuance of our first report, that Saudi Arabia would "prosecute the guilty to the fullest extent of the law."[11]

6. *Saudi Arabia continues to export radical extremism.* A battle of ideas undergirds the global war on terrorism. Militant groups such as al-Qaeda are fueled by uncompromising fundamentalist interpretations of Islam that espouse violence and that millions of Muslims, Christians, and Jews reject.

   As a core tenet of its foreign policy, Saudi Arabia funds the global propagation of Wahabism, a brand of Islam that, in some instances, supports militancy by encouraging divisiveness and violent acts against Muslims and non-Muslims alike. We are concerned that this massive spending is helping to create the next generation of terrorists and therefore constitutes a paramount strategic threat to the United States. Through the support for *madrassas*, mosques, cultural centers, hospitals, and other institutions, and the training and export of radical clerics to populate these outposts, Saudi Arabia has spent

[11] We note that Saudi Arabia is not alone in failing to incarcerate Specially Designated Global Terrorists. Yousef Nada, for example, the founder of Bank Al Taqwa, remains free in Switzerland. According to U.S. officials, Bank Al Taqwa provided financial and other services to al-Qaeda and Hamas, and Nada, a senior member of the Muslim Brotherhood, provided financial assistance to Osama Bin Laden and al-Qaeda following the terrorist attacks of September 11, 2001.

what could amount to hundreds of millions of dollars around the world financing extremism.[12]

We recognize the complexity associated with making policy recommendations concerning this activity, which is motivated in large part by deeply held religious principle. We have no doubt that this financing has in many instances improved the human condition in hard-pressed corners of the world, providing aid and comfort to orphans, widows, refugees, the hungry, the sick, and the infirm. But precisely because religious impulses undergird support for such financing, it is not necessarily "no strings attached" assistance.[13] Rather, it is inextricably tied to the global spread of Wahabism, in both Muslim and non-Muslim countries.[14] As a result, because it frequently is intended to, and does in fact, propagate extremism in vulnerable populations, this spending is fundamentally problematic from the standpoint of U.S strategic interests. We find that it must be directly, immediately, and unequivocally addressed.

Such Saudi financing is contributing significantly to the radicalization of millions of Muslims in places ranging from Pakistan to Indonesia to Nigeria to the United States. Foreign funding of extremist *madrassas* in Pakistan alone, for example, is estimated in the tens of millions, much of it historically from Saudi Arabia. Saudi patronage has played an important role in promoting *jihadi* culture in Pakistan, including through extensive assistance to Ahl-e Hadith (Salifi/Wahabi) *madrassas*. More than a million young Pakistanis are educated in these *madrassas*, according to a recent report co-sponsored by the Council on Foreign Relations and the Asia Society.[15] Islamic religious schools in Afghanistan, India, Yemen, Africa, Central Asia, the Balkans (particularly

---

[12] Estimates of Saudi charitable spending are difficult to come by. According to the Charity Report issued by the Saudi government on April 21, 2002, Saudi Arabia has spent over $24 billion on charitable causes since 1970. In June 2004, Adel al Jubeir, foreign policy adviser to the crown prince, estimated that Saudi charities disbursed approximately $100 million per year, which could double or triple as circumstances warranted. We are by no means suggesting that all or even a majority of this spending is financing terrorism or extremism.

[13] As the May 2003 report of the U.S. Commission on International Religious Freedom notes, "The Saudi government also funds numerous relief organizations that provide humanitarian assistance, but which also have propagation as a component of their activities."

[14] Although reliable data concerning these activities are hard to come by, we attach as Appendix B official Saudi data detailing some such efforts in non-Muslim countries.

[15] *New Priorities in South Asia: U.S. Policy Toward India, Pakistan, and Afghanistan*, Chairmen's Report of an Independent Task Force Co-Sponsored by the Council on Foreign Relations and the Asia Society (2003). See also *Pakistan: Madrasas, Extremism and the Military*, International Crisis Group Asia Report No. 36, July 29, 2002.

Bosnia and Kosovo), North America, Chechnya, and Dagestan are also significantly financed by Saudi sources.

This massive spending is an integral part of the terrorist financing problem. It fosters virulence and intolerance directed against the United States, Christians, Jews, and even other Muslims. The May 2003 report of the U.S. Commission on International Religious Freedom notes, "Many allege that the kind of religious education propagated in Saudi-funded Islamic schools, mosques, and Islamic centers of learning throughout the world fuels hatred and intolerance, and even violence, against both Muslims and non-Muslims. Some Saudi government-funded textbooks used both in Saudi Arabia and also in North American Islamic schools and mosques have been found to encourage incitement to violence against non-Muslims. There have also been reports that some members of extremist and militant groups have been trained as clerics in Saudi Arabia; these groups promote intolerance of and even violence against others on the basis of religion."

Saudi Arabia has begun to crack down on *domestic* extremism, most dramatically through education reform and the banishment or "re-education" of scores of radical Wahabi clerics. But we find that there is less evidence of effective action to curb the ongoing *export* of extremism. The Saudi Ministry of Islamic Affairs, for example, continues to provide inflammatory materials and clerics outside the Kingdom. The ministry has offices in every Saudi embassy and relies on its own funds rather than a central budget, giving it an important degree of operational autonomy. Saudi Arabia has begun to scrutinize more closely, and in some cases recall, its Islamic attaches. More comprehensive vetting, faster action, and greater policy clarity is necessary.[16]

The overseas branches of Saudi-based charities are another key link in this chain. According to a March 2003 State Department report, "Hundreds of millions of dollars in charitable donations leave Saudi Arabia every year and, wittingly or unwittingly, some of these funds have been channeled to terrorist organizations." Although, as discussed above, Saudi Arabia has introduced new legal, regulatory, and institutional reforms

[16] It is not clear, for example, whether and to what extent Islamic Affairs offices are being closed down internationally as a matter of policy. From October 2003 to late January 2004, individuals associated with Islamic Affairs activities in the United States and who previously held Saudi diplomatic credentials left the United States. In December 2003, a Saudi official remarked, "We are going to shut down the Islamic affairs section in every embassy." In January 2004, the Minister of Islamic Affairs responded, "the [Islamic Affairs] centers are working and they are part of the Kingdom's message."

intended to regulate and control these disbursements, the recent evidence of effective enforcement action against wayward overseas branches is not encouraging, and there have continued to be concerns regarding the flow of private funds to them.

Halting efforts to reform or close branches of the Al Haramain Islamic Foundation, one such charity, offer a case in point. Even before September 11, U.S. investigators had tied the Tanzanian branch of Al Haramain to the 1998 bombings of the U.S. embassies in Nairobi and Dar es Salaam. According to its founder, Al Haramain has built 1,300 mosques, sponsored 3,000 preachers, and produced twenty million religious pamphlets since its founding. According to the Treasury Department, "When viewed as a single entity, AHF is one of the principal Islamic NGOs providing support for the al-Qaeda network and promoting militant Islamic doctrine worldwide."

In March 2002, Saudi Arabia, in a joint enforcement action with the United States, announced that the closure of the Bosnia and Somalia branches of Al Haramain. By October 2002, the Bosnia branch was reportedly back in operation, building a $530,000 Islamic Center in Sarajevo. After months of pressure from the United States, Saudi Arabia agreed last winter to restructure Al Haramain and to put in place a new board and management. Following the May 12 Riyadh bombings, the Saudis agreed to close additional branches of Al Haramain in places such as Pakistan, Kosovo, Indonesia, Kenya, Ethiopia, and Tanzania. In July 2003, the *New York Times* reported that the once-closed Indonesia affiliate was back in operation. And on December 22, 2003, the United States and Saudi Arabia jointly designated Vazir, which turned out to be the successor to the previously designated Al Haramain-Bosnia. On January 22, 2004, the United States and Saudi Arabia jointly proposed to the UN's al-Qaeda and Taliban Sanctions Committee Al Haramain branches located in Indonesia, Kenya, Tanzania, and Pakistan, which the two governments said provided financial, material, and logistical support to the al-Qaeda network and other terrorist organizations and which the Saudi government had said in 2003 would be closed. On February 18, 2004, a federal search warrant was executed against property purchased on behalf of an Ashland, Oregon, affiliate of Al Haramain, and its accounts were blocked. On June 2, 2004, the United States and Saudi Arabia announced the designation of five additional branches of Al Haramain located in

Afghanistan, Albania, Bangladesh, Ethiopia, and the Netherlands. More significantly, Saudi Arabia announced the dissolution of Al Haramain.

Remarkably, no one has gone to jail for allowing Al Haramain to be used as a financial conduit for terrorism, although earlier this year it was announced that the founder and leader of Al Haramain—Aqeel Abdulaziz Al-Aqil—stepped down from his post, and was replaced by his deputy. Before doing so, he asserted last June, without public contradiction by Saudi officials, that his organization has done nothing wrong: "It is very strange that we are described as terrorist..... Maybe there has been a mistake."

We also note that more recently the United States has formally designated Al-Aqil as an individual supporting terrorism, but Saudi Arabia has thus far refused to take this action.

Enforcement action against Al Haramain took too long and was frustrated by lethargy and half-steps. Al Haramain, moreover, is only of one of a handful of large Saudi-based charities fueling extremism; some half a dozen others, including some of the largest and most visible, such as the International Islamic Relief Organizatiom (IIRO) and the World Assembly of Muslim Youth (WAMY), have repeatedly been linked to global terrorist organizations.[17] We welcome the announced dissolution of Al Haramain and look forward to the prompt dissolution of other large Saudi-based charities tied to the support of global terrorist organizations.

Although the United States is not and should not be at war with any religion or any religious sect, we find that U.S. policy should affirmatively seek to drain the ideological breeding grounds of Islamic extremism, financially and otherwise.[18] To do so, we will

[17] For example, Kenyan security authorities reportedly expelled the IIRO from Kenya following the 1998 bombings of the U.S. Embassies in Nairobi and Dar es Salaam for "working against the interests of Kenyans in terms of security." Since then, IIRO has also reportedly been accused by U.S. and Philippine officials of serving as a conduit for funding the militant Abu Sayyaf Group. Similarly, WAMY has reportedly directed funds to Pakistani-backed terrorists in Kashmir. WAMY has also reportedly been under federal investigation in the United States for its alleged involvement in terrorist financing activities.

[18] In this regard, we agree with the following observation of the May 2003 report of U.S. Commission on International Religious Freedom: "The Commission is concerned about numerous credible reports that the Saudi government and members of the royal family directly and indirectly fund the global propagation of an exclusivist religious ideology, Wahhabism, which allegedly promotes hatred, intolerance, and other abuses of human rights, including violence. The concern is not about the propagation of Islam *per se*, but about allegations that the Saudi government's version of Islam promotes abuses of human rights, including violent acts, against non-Muslims and disfavored Muslims. The concern is broader than the allegation that the Saudi government is supporting and financing terrorism, which has received substantial attention following the September 11, 2001, terrorist attacks in the United States." See also the Commission's 2004 report and statements.

need more demonstrable cooperation from Saudi Arabia, which so far as not been sufficiently forthcoming.

7. *The Executive Branch has not widely used the authorities given to it in the USA PATRIOT Act to crack down on foreign jurisdictions and foreign financial institutions suspected of abetting terrorist financing.* In our first report, we urged the U.S. government to make use of the new powers given to the secretary of the Treasury to designate individual foreign jurisdictions or foreign financial institutions as being of "primary money laundering concern" to the United States and thereby impose "special measures" that could include cutting off such jurisdictions or banks from U.S. financial markets. At the time of our initial report, those authorities had never been used or even publicly threatened, notwithstanding their obvious potential effectiveness in affecting the behavior of recalcitrant states or financial institutions. Soon after the issuance of our initial report, the U.S. government announced its intention to impose "special measures" against Nauru and Ukraine and, in November 2003, its intention to impose "special measures" against Burma and two Burmese banks—all of which, in our judgment, are appropriately designated as being of "primary money laundering concern" to the United States, but none of which is a modality of terrorist financing. As this report was going to press, the Bush administration used "special measures" for the first time in a terrorist financing context, against a Syrian bank and its Lebanese subsidiary. Several times since we made our October 2002 recommendation, senior officials of the Bush administration have stated, both publicly and privately, that they were considering the wider use of "special measures" in connection with the financing of terrorism—but to date the Bush administration has not used this powerful tool to combat terrorist financing, with the exception of its actions against the Syrian bank and its Lebanese subsidiary noted above. With recent changes to the law that will protect from disclosure classified information used as a basis for such designations, we anticipate, and again strongly urge, the increased use of "special measures," particularly against problematic foreign financial institutions.
8. *Global coordination to curtail the financing of Hamas is inadequate.* Targeting the financial support network of Hamas is an important part of the overall war on terrorist financing, affecting both the Middle East peace process and the larger U.S.-led war on

terrorism. However, in Saudi Arabia, whose people and organizations may contribute as much as 60 percent of Hamas's annual budget, the government still does not recognize Hamas as a terrorist organization, notwithstanding important recent steps, such as the announced cessation of official efforts to raise money for the families of Palestinian suicide bombers. In this respect, Saudi actions and opinions are widely mirrored throughout Arab and Muslim communities around the world. Even if official support and telethons have stopped, much more needs to be done to monitor the disbursement of private funds.

The EU has now officially added Hamas to its list of terrorist groups. But to date, the EU has designated only a small number of Hamas-affiliated entities. Britain and only a handful of other European states have joined U.S.-led enforcement actions against Hamas leaders and fronts, although Britain has not yet taken effective action to close the Palestinian Relief and Development Front (Interpal), perhaps the largest Hamas front organization in Europe. No such action has been taken by other European countries that are home to other Hamas front organizations, such as Austria, France, and Italy. The EU's decision to ban Hamas will remain meaningless until such time as the EU and its constituent member states act aggressively to restrict Hamas financial activities to the maximum extent possible.

RECOMMENDATIONS

As a general matter, we wish to reaffirm the principal recommendations of our initial report, reproduced here in Appendix A.[19] With our new "findings" in mind, we wish to make the following additional recommendations:

1. *U.S. policymakers should seek to build a new framework for U.S.-Saudi relations.* The Task Force recognizes the broader context of the complex and important bilateral relationship in which the terrorist financing issue is situated. The U.S.-Saudi relationship implicates many critical U.S. interests, including energy security, Iraq, the Middle East peace process, and the broader war on terrorism. And although most of us are not regional experts, we do have experience working on issues of bilateral concern and we feel competent to offer a perspective on U.S.-Saudi relations based on the manner in which Saudi financial support for terrorism—one of the most important issues in that relationship—has been addressed or avoided by both countries.
    a. For decades, presidents of both parties built U.S.-Saudi Arabia relations upon a consistent framework understood by both sides: Saudi Arabia would be a constructive actor with regard to the world's oil markets and regional security issues, and the United States would help provide for the defense of Saudi Arabia, work to address the Israeli-Palestinian conflict, and not raise any significant questions about Saudi Arabian domestic issues, either publicly or privately. For decades, this unarticulated framework held despite its inherent tensions. It broadly served the interests of both the U.S. and Saudi Arabian governments.
    b. Since then, however, al-Qaeda, a terrorist organization rooted in issues central to Saudi Arabian domestic affairs, has murdered thousands of Americans and

[19] Some of our initial recommendations have been overtaken by events or otherwise require modification owing to the passage of time. In our initial recommendations, for example, we suggested that banks should build specific anti-terrorist financing compliance components and avail themselves of public and private sources of information that identify persons or institutions with links to terrorist financing. As is suggested by our current recommendation seven, the most viable means by which banks can identify persons or institutions that may have links to terrorist financing is for the government to provide relevant information to banks. Extensive work by banks, in coordination with the government, has not yielded any specific anti-terrorist financing compliance tools that will assist banks in identifying persons or institutions related to terrorist financing. Similarly, banks have not been able to rely solely or effectively on public and private sources of information as such information is extremely diverse and often times either inaccurate or not sufficient to provide any meaningful assistance.

conspires to kill even more. Thus changing circumstances have called into question at least one key tenet of the historical framework for U.S.-Saudi relations. When domestic Saudi problems threaten Americans at home and abroad, a new framework for U.S.-Saudi relations must be struck, one that includes focused and consistent U.S. attention on domestic Saudi issues that previously would have been "off the table."

c. This evolution is already underway, as evidenced by new tensions in the bilateral relationship since 9/11. We believe that U.S.-Saudi relations can and should come to resemble more closely U.S. bilateral relations with other large, important regional powers with which the United States has a complex pattern of bilateral relations and where domestic issues are always "on the table," often to the consternation of the other party. China and Russia (and before it, the Soviet Union) have been forced to confront domestic issues they would otherwise ignore in the context of their bilateral relations with the United States. Consistent U.S. demands for human rights and political and economic freedom in these places may only have or have had a marginal impact on the course of events, but they are a fundamental expression of U.S. interests and values. And just as U.S. demands on China and Russia have become a challenging but fundamentally manageable (and constructive) aspect of our diplomacy, so too will U.S. demands regarding Saudi "domestic" issues like terrorist financing and the global export of Islamic extremism.[20]

d. More immediately, both U.S. policymakers and the American people should fully recognize the significance of what is currently taking place in Saudi Arabia. After the bombings this April, Prince Bandar, the Saudi ambassador to the United States, declared that "it's a total war with them now." Some Bush administration officials have privately characterized the current state of affairs as a "civil war" and suggested that the appropriate objective for U.S. policy in this context is to

[20] In this regard, we agree with the approach proposed in May 2003 by the U.S. Commission on International Religious Freedom for reformulating the U.S.-Saudi relationship: "As with other countries where serious human rights violations exist, the U.S. government should more frequently identify these problems and publicly acknowledge that they are significant issues in the bilateral relationship." See also the Commission's 2004 report and statements. We believe that such a declaratory approach should extend beyond human rights issues to include specifically the issues within the mandate and expertise of this Task Force.

help the current regime prevail. We agree, but we also believe that this perspective does not go far enough.

e. Under this view, the domestic Saudi problem is conceived primarily in terms of the presence of a certain number of al-Qaeda cells and members in Saudi Arabia. When they have been discovered and dispatched, the problem will be over and the "civil war" will be won. In our view, the current al-Qaeda problem in Saudi Arabia will not be won by eliminating a certain number of terrorists; rather, victory will only be achieved when the regime finally decides to confront directly and unequivocally the ideological, religious, social, and cultural realities that fuel al-Qaeda, its imitators, and its financiers all over the world. Therefore, the appropriate goal for U.S. foreign policy is for the Saudi regime to win their civil war—and to change responsively and fundamentally in the process.

2. *Saudi Arabia should fully implement its new laws and regulations and take additional steps to further improve its efforts to combat terrorist financing.* Saudi Arabia should take prompt action to implement fully its new laws and regulations. It should deter the financing of terrorism by publicly punishing those Saudi individuals and organizations who have funded terrorist organizations. It should increase the financial transparency and programmatic verification of its global charities. And it should publicly release audit reports of those charities that are said to have been completed.

   a. Saudi Arabia should ratify and implement treaties that create binding international legal obligations relating to combating money laundering and terrorist financing, including the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism and the 2000 UN Convention against Transnational Organized Crime (Palermo Convention).

3. *Multilateral initiatives must be better coordinated, appropriately funded, and invested with clear punitive authorities.* The need for a new international organization specializing in terrorist financing issues, as recommended by our initial report, has diminished as a result of significant efforts being undertaken by a variety of international actors. The need for proper coordination and clearer mandates has increased for the same reason. Duplicative efforts should be minimized and resources reallocated to the most logical lead organization.

a. For example, coordinated efforts among the CTC, the CTAG, the IMF, and the World Bank will be necessary to assess and deliver capacity-building assistance with efficiency. Such assistance is critical. Substantial progress has been made in many countries to put in place legal authorities to criminalize terrorist financing and to act expeditiously to freeze funds. But in many places, a lack of technical capacity inhibits the ability of member states to comply fully with the U.S.-led multilateral sanctions regime. The vast majority of financial institutions in these states still lack the ability to identify and block—effectively, efficiently, or at all—designated financial or non-financial assets.

b. Given the profusion of actors, clear mandates are essential. As a general matter, we believe that the CTC should lead international efforts to coordinate the delivery of multilateral capacity-building efforts. Although somewhat outside its mandate, we also believe that the CTC should lead international efforts to develop universally acceptable evidentiary, intelligence-sharing, and enforcement standards acceptable to a large number of member states, the lack of which has also impeded the effectiveness of the U.S.-led multilateral sanctions regime.

c. We believe that the FATF should lead international efforts not only to articulate international standards relating to anti–money laundering and counterterrorist financing (AML/CTF), but also to monitor and assess implementation and compliance with those standards. In order to do so, the FATF will need an expanded mandate and budget, since it currently does not normally assess implementation. It will also need to be reinvested with the political authority to "name and shame" nations that fail to adopt or implement regimes that meet international standards, as described in our initial report. In this regard, it should work closely with the CTC and the UN Security Council, which have the authority to impose sanctions on member states that fail to comply with mandatory international legal obligations relating to terrorist financing.

d. FATF's resources should also be expanded to allow it to spearhead additional initiatives in the global campaign against terrorist financing, including those relating to the regulation of charities and *hawala* and, as described in our initial report, the creation and promulgation of global "white lists" of financial

institutions and charities that conform to the highest compliance standards, regardless of the legal environment in their home jurisdictions. Additional resources for FATF might be found by reprogramming resources from other international organizations performing similar or redundant assessment functions.

4. *The Bush administration should formalize its efforts to centralize the coordination of U.S. measures to combat terrorist financing.* Our last report criticized the organizational structure then being used to coordinate U.S. diplomatic, intelligence, regulatory, and law enforcement policies and actions. Although organizational in nature, this was a core recommendation of our last report, since from good organization comes good policy. Our understanding is that, in practice, responsibilities for this coordination have since shifted from the Treasury Department to the White House, as we recommended in our original Task Force report. However, while outgoing Deputy National Security Adviser Frances Townsend has led interagency efforts and critical delegations abroad, there has been no formal designation of which we are aware of her or her office's lead role. That should happen forthwith, in the form of a National Security Presidential Directive (NSPD) or otherwise. Given Townsend's imminent departure, the usual bureaucratic realities of Washington, and the unique complexity of the terrorist financing issue—compounded by dislocations caused by the birth of the Department of Homeland Security, the resulting elimination of the Treasury Department's historical enforcement function, and the Treasury Department's more recent announcement of the creation a new Undersecretary for Terrorism and Financial Intelligence—such clarity is needed. The unusually rapid turnover seen in senior White House personnel responsible for counterterrorism makes it even more critical that such a clear designation is made, so leadership on this issue becomes a matter of institutional permanence rather than a function of individual personalities and relationships. Moreover, such a designation will go a long way toward putting issues regarding terrorist financing front and center in every bilateral diplomatic discussion with every "frontline" state in the fight against terrorism—at every level of the bilateral relationship, including, on a consistent basis, the highest.
5. *Congress should enact a Treasury-led certification regime on terrorist financing.* Many countries have taken steps to improve their anti–money laundering and counterterrorist fighting regimes, but many have not. Certification regimes can be controversial and are

occasionally inefficient, and they frequently become a bone of contention with foreign governments that do not wish to be seen as giving in to congressional or more broadly U.S. pressure. Nevertheless, they also have the ability to galvanize quickly action consistent with U.S. interests. Moreover, they require official findings of fact that have the effect of compelling sustained U.S. attention to important topics that, on occasion, U.S. officials find it more expedient to avoid. For these reasons, we believe that Congress should pass and the president should sign legislation requiring the executive branch to submit to Congress on an annual basis a written certification (classified if necessary) detailing the steps that foreign nations have taken to cooperate in U.S. and international efforts to combat terrorist financing. Within the executive branch, this certification process is naturally led not by the State Department but by the Treasury Department, which has the deepest expertise and is on the frontlines of broader U.S. efforts. Such a regime would otherwise be similar to the State Department-led regime that is currently in place to certify the compliance of foreign nations with U.S. and international counternarcotics efforts and should appropriately take into account the capacity and resources available to states subject to the regime. In the absence of a presidential national security waiver, states that cannot be so certified would be subject to sanctions, including the revocation or denial of U.S. foreign assistance monies and the restriction or denial of access to the U.S. financial system pursuant to Section 311 of the USA Patriot Act or the International Emergency Economic Powers Act. As outlined in Section 311, and as discussed in depth in our previous report, these authorities are examples of "smart sanctions," allowing the U.S. government to target specific foreign institutions or classes of transactions, as well as entire foreign jurisdictions.

6. *The UN Security Council should broaden the scope of the UN's al-Qaeda and Taliban Sanctions Committee to include the development of a comprehensive list of sanctioned international terrorist organizations and associated entities—including specifically Hamas and its fronts, among others.* Rather than focusing exclusively on entities related to the Taliban and al-Qaeda, the Sanctions Committee should explicitly designate other groups utilizing terrorism transnationally or globally that constitute a threat to international peace and security. The UN Security Council should specifically impose international sanctions on other groups and individuals that have been designated as

terrorists, as Hamas has been by the United States and EU, and require, as a matter of international law, that member states take enforcement action against such entities designated by the Sanctions Committee. The enabling resolution for these expanded authorities should explicitly reject the notion that acts of terror may be legitimized by the charitable activities or political motivations of the perpetrator. No cause, however legitimate, justifies the use of terror; indeed, the use of terror delegitimizes even the most worthy causes.

7. *The U.S. government should improve the flow of information to financial services sector pursuant to Section 314 of the USA PATRIOT ACT.* International financial institutions subject to U.S. jurisdiction are among our best sources of raw financial intelligence—if they know what to look for. Section 314(a) of the USA PATROIT ACT requires the Treasury Department to promulgate regulations "to encourage further cooperation among financial institutions, their regulatory authorities, and law enforcement authorities, with the specific purpose of encouraging regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities." These procedures are not working as effectively as they might, and very little information flows back from the government to financial institutions that spend considerable resources on compliance programs that they wish to be effective. Accelerated efforts are necessary to make operational Section 314 of the USA PATRIOT ACT, so that financial institutions are best able to marshal their considerable resources and expertise in furtherance of the national interest. This should include the further exploration of ways to share classified information with the private sector and to ensure that relevant information is not overclassified. Civilian employees of other private sector enterprises impacting national security—such as the defense and transportation industries—receive sensitive information, and there is no reason why employees of U.S. financial services firms cannot do so as well.
8. *The National Security Council and the White House Office of Management and Budget (OMB) should conduct a cross-cutting analysis of the budgets of all U.S. government agencies as they relate to terrorist financing.* Because we do not today have a clear sense

of how many financial and human resources are actually devoted to the various tasks involved in combating terrorist financing, it is impossible to make fully informed, strategic decisions about whether functions are duplicative or resource allocations are optimal. For this reason, the NSC and OMB should conduct a cross-cutting analysis of all agencies' budgets in this area, to gain clarity about who is doing what, how well, and with what resources. Provision should be made to incorporate classified material, so that the full range of activity underway is considered: (1) intelligence collection, analysis, and operations; (2) law enforcement operations (including related operations against money laundering, drug trafficking, and organized crime); (3) regulatory activity, including policy development, enforcement, and international standard setting and implementation; (4) sanctions, including an analysis of their effectiveness as an interdiction and deterrence mechanism; (5) diplomatic activity in support of all of the above; and (6) contributions made by the Defense Department. Only with such a cross-cut in hand can we can begin to make assessments regarding the efficiency of our existing efforts and the adequacy of appropriations relative to the threat.

9. *The U.S. government and private foundations, universities, and think tanks in the United States should increase efforts to understand the strategic threat posed to the United States by radical Islamic militancy, including specifically the methods and modalities of its financing and global propagation.* At the dawn of the Cold War, the U.S. government and U.S. nongovernmental organizations committed substantial public and philanthropic resources to endow Soviet studies programs across the United States. The purpose of these efforts was to increase the level of understanding in this country of the profound strategic threat posed to the United States by Soviet Communism. A similar undertaking is now needed to understand adequately the threat posed to the United States by radical Islamic militancy, along with its causes, which we believe constitutes the greatest strategic threat to the United States at the dawn of this new century. This national undertaking should specifically include study and analysis of the financial and other means by which this threat to the United States is propagated, concerning which almost no reliable data is publicly available. In this regard, we endorse the May 2003 recommendation of the U.S. Commission on International Religious Freedom (reaffirmed in 2004) that Congress initiate and make public a study on Saudi exportation of

intolerance, to include, from the Saudi government, "an accounting of what kinds of Saudi support go to which religious schools, mosques, centers of learning and other religious organizations globally." We also endorse steps taken in recent weeks by the General Accounting Office to implement this recommendation. To be commensurate with the threat, much more will need to be done, not only in Washington, but also by private foundations, universities, and think tanks, in a more sustained, deliberate, and well-financed manner than that afforded through ad hoc initiatives such as this Task Force.

MEMBERS OF THE TASK FORCE

THOMAS J. BIERSTEKER, Henry R. Luce Professor and Director, Watson Institute, Brown University

RICHARD A. CLARKE, Chairman, Good Harbor Consulting, LLC; former National Coordinator for Security, Infrastructure Protection and Counterterrrorism, the White House

DAVID COHEN, Deputy Commissioner for Intelligence, New York City Police Department; former Deputy Director for Operations, Central Intelligence Agency

W. BOWMAN CUTTER, Managing Director, Warburg Pincus; former Deputy Assistant to the President for Economic Affairs

STUART E. EIZENSTAT, Partner, Covington & Burling; former Deputy Secretary of the Treasury, Under Secretary of State, and U.S. Ambassador to the European Union

MALLORY FACTOR (vice chair), Chairman, MALLORY FACTOR INC

MICHAEL R. FENZEL, Chairman, Council for Emerging National Security Affairs (CENSA); former Director for Transnational Threats, National Security Council

MAURICE R. GREENBERG (chair), Chairman and CEO, American International Group

GEOFFREY KEMP, Director, Regional Strategic Programs, The Nixon Center; former Senior Director, Near East & South Asian Affairs, National Security Council

MATTHEW LEVITT, Senior Fellow, Washington Institute for Near East Policy; former counterterrorism analyst, Federal Bureau of Investigation

STEWART J. PAPERIN, Executive Vice President, Soros Foundations

RICHARD A. SMALL, Managing Director, Global Anti–money Laundering, Citigroup; former Deputy Associate Director, Board of Governors of the Federal Reserve System

MAURICE SONNENBERG, Senior International Adviser, Bear, Stearns & Co.; Senior International Adviser, Manatt Phelps & Phillips, LLP; former Vice Chairman, National Commission on Terrorism

TODD D. STERN, Partner, Wilmer Cutler Pickering Hale and Dorr, LLP; former Counselor to the Secretary of the Treasury and Staff Secretary, the White House

WILLIAM F. WECHSLER (co-director), Vice President, Greenwich Associates; former Director for Transnational Threats, National Security Council, and Special Adviser to the Secretary of the Treasury; former chair of the interagency group charged with disrupting al-Qaeda's financial network

JONATHAN WINER, Partner, Alston & Bird; former Deputy Assistant Secretary of State for International Law Enforcement Affairs

LEE S. WOLOSKY (co-director), Of Counsel, Boies, Schiller & Flexner, LLP, and Adjunct Professor of International Affairs, Columbia University; former Director for Transnational Threats, National Security Council

OBSERVER TO THE TASK FORCE

HEATHER K. KIRIAKOU, Visiting Fellow, Council on Foreign Relations

---

Note: Institutional affiliations are for identification purposes only.

APPENDIX A

PRINCIPAL FINDINGS AND RECOMMENDATIONS OF OCTOBER 2002 TASK FORCE REPORT ON TERRORIST FINANCING

FINDINGS

1. The Task Force recognizes and welcomes the recent progress that has been made in combating terrorist financing, both at home and abroad. It congratulates Congress and the Bush administration—and President Bush personally—for focusing on this issue, particularly in the immediate wake of the September 11 terrorist attacks.
2. Notwithstanding substantial efforts, the Task Force finds that currently existing U.S. and international policies, programs, structures, and organizations will be inadequate to assure sustained results commensurate with the ongoing threat posed to the national security of the United States. Combating terrorist financing must remain a central and integrated element of the broader war on terrorism
3. Two administrations have now grappled with this difficult, cross-cutting problem. Neither has found a single "silver bullet," because none exists. Given the very nature of the problem, it must be continually "worked" rather than "solved."
4. Gaining international cooperation though a mix of incentives and coercion is a necessary prerequisite for progress. Effective international efforts will require strong U.S. leadership.
5. Deficiencies in political will abroad—along with resulting inadequacies in regulatory and enforcement measures—are likely to remain serious impediments to progress. One-time affirmations cannot substitute for sustained enforcement, regulatory, and institution-building measures.
6. In the short term, "following the money" can go a long way toward disrupting terrorist cells and networks and thereby help prevent future terrorist attacks. But real and sustainable success will be achieved only over the very long term, as key countries make fundamental changes to their legal and regulatory environments.
7. Long-term success will depend critically upon the structure, integration, and focus of the U.S. government—and any intergovernmental efforts undertaken to address this problem.

RECOMMENDATIONS

With these findings in mind, the Task Force makes the following core structural recommendations:

1. *The president should designate a Special Assistant to the President for Combating Terrorist Financing with the specific mandate to lead U.S. efforts on terrorist financing issues.* Such an official would direct, coordinate, and reaffirm the domestic and international policies of the United States on a day-to-day basis and with the personal authority of the president of the United States. He or she would report to the president through the national security adviser. In addition, he or she would serve as sous-sherpa to the G-7 and chief U.S. representative to all important regional organizations with respect to terrorist financing issues once they are made permanent agenda items as described below. He or she would be responsible for implementing the strategic and tactical recommendations contained in this report and leading U.S. efforts with respect to the international initiatives described below.
2. *The United States should lead international efforts, under the auspices of the G-7, to establish a specialized international organization dedicated solely to investigating terrorist financing.* Such an organization would assume ad hoc terrorist financing-related initiatives undertaken by the FATF since September 11, 2001, and support and reinforce the activities of the UN Counter-Terrorism Committee undertaken since that time to coordinate and assist in the implementation of member states' obligations under Security Council resolutions pertaining to terrorist financing. Membership in this specialized organization could initially be limited to the G-7 itself, an approach similar to that taken by the G-8 in 1994 in forming the Lyons Group against international crime. Membership could then be expanded to include other states with highly developed financial regulatory and enforcement systems that are committed to the top-down promulgation of the most stringent international standards to combat terrorist financing. This new organization would be tasked with the implementation of the *multilateral* initiatives described below. (See Section II: Recommendations Applicable to the International Community).

I. RECOMMENDATIONS APPLICABLE TO THE UNITED STATES

Strategic

1. Put issues regarding terrorist financing front and center in every bilateral diplomatic discussion with every "front-line" state in the fight against terrorism—at every level of the bilateral relationship, including the highest. Where sufficient progress is not forthcoming, speak out bluntly and forcefully about the specific shortfalls in other countries' efforts to combat terrorist financing. The Task Force appreciates the necessary delicacies of diplomacy and notes that previous administrations also used phrases that obfuscated more than they illuminated when making public statements on this subject. Nevertheless, when U.S. spokespersons are only willing to say that "Saudi Arabia is being cooperative" when they know very well all the ways in which it is not, both our allies and adversaries can be forgiven for believing that the United States does not place a high priority on this issue.
2. Reconsider the conceptually flawed "second phase" policy that (1) diminishes the likelihood of additional U.S. designations under IEEPA of foreign persons and institutions with ties to terrorist finances, and (2) relies on other countries for leadership, a role they are not suited for nor willing to play. IEEPA designations and blocking orders—actual or threatened—are among the most powerful tools the United States possesses in the war on terrorist finances. The United States should not relinquish them, nor should the United States relinquish U.S. leadership to coalition partners uninterested or unsuited for this role.
3. As an example to U.S. friends and allies, bring *hawaladars* and other underground money service businesses fully into the federal regulatory system. During both the Clinton and Bush administrations, FinCEN has been very slow in its efforts to register *hawaladars*. There is currently no federal plan to coordinate federal, state, and local law enforcement efforts to identify, surveil, and prosecute unregistered *hawaladars*. FinCEN should immediately make its register of money services businesses available online, to facilitate the use of the information by federal, state, and local law enforcement agencies seeking to determine the legality of local money changers' and money transmitters' operations.

Similarly, as a further example to the United States' friends and allies, require charities operating in the United States to abide by certain U.S. anti–money laundering laws, by, for example, having the Treasury Department define them as "financial institutions" for purposes of implementing any "special measures" put in place pursuant to the Patriot Act.

4. Expand U.S. bilateral technical assistance programs in problem countries to assist in the creation of effective regulatory, enforcement, and control regimes for financial institutions and charitable organizations. The president's fiscal year 2003 budget includes only $4 million for the Treasury Department's Office of Technical Assistance to provide training and expertise to foreign governments to combat terrorist financing; funding for such efforts should increase at least tenfold. Rather than being distributed directly to individual providers, such funds should be centralized and then distributed to appropriate providers, consistent with priorities established by an interagency process. Integration and coordination of such assistance is vital so that such assistance reflects administration policy. The United States should urge other nations with developed financial regulatory infrastructures, and the IMF and World Bank, to provide similar assistance.
5. Immediately develop and implement a comprehensive plan to vet and conduct background investigations on institutions, corporations, and nongovernmental organizations that receive U.S. government grant funding to ensure that U.S. funds are not diverted to organizations that either have links to terrorist groups or a history of supporting terrorist aims.
6. For the first time, make use of the new powers given to the secretary of the Treasury under the Patriot Act to designate individual foreign jurisdictions or financial institutions as being of "primary money laundering concern" to the United States, and thereby impose sanctions short of full IEEPA blocking orders. These sanctions could include cutting off correspondent relations between foreign financial institutions with weak anti–money laundering practices and U.S. banks. Unlike IEEPA, these "special measures" do not require presidential action and do not require the United States to prove a specific connection to terrorism, only that the jurisdictions or institutions targeted do not have adequate anti–money laundering controls—a much lower hurdle.

Tactical

1. Create streamlined interagency mechanisms for the dissemination of intelligence, diplomatic, regulatory, and law enforcement information. All information relating to terrorist financing—regardless of its source—should be centrally analyzed and distributed to *all* relevant policymakers. The formation of the CIA-based Foreign Terrorist Asset Tracking Group is a good start, but adequate budgets should be requested, and intelligence agencies will need to build up the level of linguistic, financial, and cultural expertise to investigate and combat Islamic terrorist financing effectively.
2. Broaden U.S. government covert action programs to include the disruption or dismantling of financial institutions, organizations, and individuals knowingly facilitating the financing of terror. Information warfare—computer hacking—and other forms of disruption should be considered when intelligence compellingly demonstrates that foreign financial institutions are knowingly and actively participating in the financing of terrorism.
3. Reinvigorate U.S. intelligence and law enforcement capacities against terrorist finance by further strengthening FinCEN. As the financial intelligence unit for the United States, FinCEN needs to be able to play a significant role in terrorist finance intelligence and analysis; liaise with other financial intelligence units (FIUs) and with domestic and international training and institution building efforts to combat terrorist finance; and play a role in international regulatory harmonization. The administration should act promptly to strengthen FinCEN's funding, personnel, and authorities to make it possible for FinCEN to perform these roles.
4. Assure the full implementation of the provisions of the Patriot Act intended to improve and deepen U.S. anti–money laundering capabilities.

II. RECOMMENDATIONS APPLICABLE TO THE INTERNATIONAL COMMUNITY

Multilateral

1. The new international organization dedicated solely to issues involving terrorist financing would be tasked with the implementation of the multilateral initiatives described below.

- Contribute to agenda-setting for the G-7 and other international and regional organizations, as described below.
- From the top down, establish strong international standards on how governments should regulate charitable organizations and their fundraising. Once those standards have been set, have technical experts publicly evaluate countries, including those in the Middle East, against them.
- Engage in similar international standard setting with regard to the regulation of *hawala*, and create and maintain a global registry of institutions that participate in *hawala* and similar alternative remittance systems.
- Work with the private and nongovernmental organization sectors to create global "white lists" of financial institutions and charities that, regardless of the legal environment in their home jurisdiction, commit to the highest due diligence, anti–money laundering, and anti–terrorist financing procedures, and agree to a system of external assessment of compliance. In addition to the reputational benefit from being included on such a "white list," inclusion on the list could be a factor taken into consideration by the World Bank, the IMF, and other international financial institutions (IFIs) in considering with which financial institutions to work. It could similarly be a factor taken into account by the U.S. Agency for International Development (USAID) and other national development and humanitarian relief agencies, as well as the United Nations High Commissioner for Refugees (UNHCR), the United Nations Development Programme (UNDP), and other multilateral agencies in determining what charities or relief organizations to work with.

- Facilitate multilateral cooperation and information sharing between the various government offices responsible for sanctions enforcement, such as the U.S. Treasury's Office of Foreign Asset Controls (OFAC). This will require each government to identify a central contact point to coordinate implementation of efforts to block terrorist finances.
- Facilitate the provision of technical assistance for all countries that need it, and further the development of the Egmont Group and capabilities to develop and share, on an intergovernmental basis, tactical financial intelligence.
- Recommend to the IMF ways in which its funding can be made contingent upon countries' implementation of strict anti–terrorist financing laws.
- Make formal recommendations to the FATF concerning which countries should be included in its "naming and shaming" processes on the basis of passive acquiescence to terrorist financing.
- Establish procedures for appeal and potential removal of the names of individuals and institutions wrongly designated as being associated with the financing of terrorism. Legitimate disquiet in some quarters concerning the potential for due process violations associated with the inaccurate listing of targeted individuals can retard progress in global efforts. Since the full sharing of sensitive intelligence information is unlikely, the establishment of such procedures will take such concerns "off of the agenda" and prevent them from being used as an excuse for inaction.

2. Terrorist financing should become a permanent agenda item of the G-7/8 and a permanent part of the agenda of all regional organizations as appropriate, such as the Association of Southeast Asian Nations (ASEAN), Asian-Pacific Economic Cooperation (APEC), and the U.S.-SADC (Southern African Development Community), among others.
3. Terrorist financing should become a permanent part of the EU-U.S. Summit agenda. EU-U.S. Summits are held twice a year and are supported by the Senior Level Group of EU and U.S. officials, which meets two or three times a semester. The Senior Level Group can and should act as a "scorecard" to monitor the progress of transatlantic cooperation.

4. Rather than superceding the FATF process of "naming and shaming" non-cooperative jurisdictions in the fight against money laundering with a "cooperative" approach, the G-7 should agree to resume and expand immediately the blacklisting of such countries. Countries on the FATF blacklist should be ineligible for certain types of IMF and World Bank lending. Once reinvigorated, the FATF needs to begin requiring full implementation and enforcement of laws and regulations, not just their passage or issuance.
5. The World Bank should provide technical assistance to less developed countries to help them establish anti–money laundering and anti–terrorist financing regimes that meet international standards.

Source and Transit Countries

Significant "source and transit" countries—especially Saudi Arabia, Pakistan, Egypt, the Gulf States, and other regional financial centers—have special responsibilities to combat terrorist financing. They should:

- Make a fundamental policy decision to combat all forms of terrorist financing and—most importantly—publicly communicate this new policy to their own nationals.
- Cooperate fully with international—especially U.S.—requests for law enforcement assistance and intelligence requests for information and other forms of cooperation. This means, among other things, allowing U.S. investigators direct access to individuals or organizations that are suspected of being involved in terrorist financing.
- Bring their bank supervision and anti–money laundering laws, regulations, and institutions completely up to international standards, and have them cover all financial institutions, including Islamic and underground ones—like the *hawala* system. Implementation of laws is necessary, not just their drafting and passage. For the most part, these countries each have the resources to do this themselves. If not, international financial and technical assistance are readily available from a variety of multilateral and bilateral

sources. The UN Counter-Terrorism Committee has compiled a directory of sources of support for this purpose.

- Require the registration and licensing of all alternative remittance mechanisms, such as *hawalas*, and close down financial institutions that fail to obtain licenses or that fail to maintain adequate customer and transaction records.
- Fully and unapologetically regulate charities subject to their jurisdiction, particularly those that serve the legitimate victims of anti-Islamic violence. Donors to legitimate charities deserve to know that their money is actually going to good causes; unknowing donors to illegitimate charities deserve to know they are being defrauded; individuals who knowingly donate to terrorist front organizations deserve to be prosecuted.
- Fully regulate the trade in gems, precious metals and other items of value regularly used to store and transfer terrorist wealth. This effort can draw on the precedents established by international efforts (what is known as the Kimberly Process) to curtail the trade in "blood diamonds."

III. NONGOVERNMENT/PUBLIC-PRIVATE

1. Recognizing that the financial services sector does not have the necessary information and intelligence to identify potential terrorists or their activities, the U.S. government should work diligently with the financial services sector to create new public-private partnerships that facilitate the sharing of intelligence information.
2. Banks and all other financial institutions should:
   - Build specific anti-terrorism financing components into their compliance and due diligence processes.
   - Utilize widely available name-recognition software to improve the efficiency of their compliance with regulatory efforts. Avail themselves of reputable public and private sources of information on the identities of persons and institutions who are suspected of links to terrorist financing and who therefore should be the subject of additional due diligence.

- Cooperate fully with any multilateral efforts to build a "white list" of institutions that have adequate anti–terrorist financing controls. A key factor for inclusion on such a list would be evidence of an institution's ability to identify and manage potential risks, such as the development and implementation of adequate anti–money laundering controls.

APPENDIX B

NEWS RELEASE

SAUDI COMMITMENT TO ESTABLISHING ISLAMIC CENTERS, MOSQUES AND INSTITUTES

Source: The Saudi Arabian Information Resource (http://www.saudinf.com/main/y3742.htm)

Riyadh, February 15, 2002

The Kingdom of Saudi Arabia has paid great attention to establishing mosques and Islamic centers, institutes and universities in a number of non-Islamic countries all over the world. Sure that this is the most effective way to spread Islamic culture and Arabic language, the Kingdom, under the leadership of the Custodian of the Two Holy Mosques, King Fahd bin Abdul Aziz, has established 210 Islamic centers in non-Islamic countries in Europe, North and South America, Australia and Asia. Among the biggest is King Fahd Islamic Center in Malaga, Spain, on an area of 3,848 sq. m., whose foundation stone was laid in 1998. The university-like Center embraces academic, educational, cultural, and propagatory activities.

King Fahd has donated five million US dollars for the cost of the Islamic Center in Toronto, Canada, in addition to 1.5 million US dollars annually to run the facility.

The Islamic Center in Brasilia; King Fahd Cultural Islamic Center in Buenos Aires; King Fahd Cultural Islamic Center in Gibraltar; King Fahd Cultural Islamic Center in Mont La Jolly, France; King Fahd Islamic Center in Edinburgh, Scotland were built at the personal expense of the Custodian of the Two Holy Mosques King Fahd bin Abdul Aziz.

The Kingdom of Saudi Arabia has also contributed to the establishment of a number of Islamic centers e.g. The Islamic Center in Geneva; Islamic Cultural Center in Brussels; Islamic Center in Madrid; Islamic Center in New York; Islamic Center in Australia; Islamic Center in Zagreb, Croatia; Cultural Center in London; Islamic Center in Lisbon, Portugal; and Islamic Center in Vienna, Austria. In Africa, the Kingdom fully financed King Faisal Center in N'djamena, Chad, and contributed to the establishment of the Islamic Center in Abuja, Nigeria, and Islamic African Center in Khartoum, the Sudan.

In Asia, the Kingdom of Saudi Arabia has fully financed King Fahd Islamic Center in the Maldives, Islamic Center in Tokyo and contributed to the establishment of the Saudi Indonesian Center for Islamic Studies in Indonesia.

The Kingdom has established more than 1,359 mosques abroad at a cost of SR 820 million, notably King Fahd Mosque in Gibraltar; Mont La Jolly Mosque in France; King Fahd Mosque in Los Angeles; King Fahd Mosque in Edinburgh, Scotland; Islamic Center Mosque in Geneva, Switzerland at a cost of SR 16 million; the 4000-worshippers-capacity Brussels Mosque at a cost of SR 20 million; and Madrid Mosque, the biggest in the West. Other mosques partially financed by the Kingdom included mosques in Zagreb, Lisbon, Vienna, New York, Washington, Chicago, Maryland, Ohio, Virginia and 12 mosques in a number of countries in south America.

In Africa, the Islamic Solidarity Mosque was established in Mogadishu, Somalia, four mosques in main cities in Gabon, two mosques in Burkina Faso, Zanzibar Mosque in Tanzania and Grand Mosque in Senegal. Among mosques which received the Kingdom's or King Fahd's personal financial support are Leon Mosque in France (SR 11 million); King Faisal Mosque in Chad (SR 60m); King Faisal Mosque in Ghenia (SR 58m); Grand Mosque in Senegal (SR 12m); Farooee

Mosque in Cameroon (SR 15.6m); Zanzibar Mosque in Tanzania (SR 10m); Bamako Mosque in ali (SR 23m); Yaoundi Mosque in Cameroon (SR 5m); al Azhar Mosque in Egypt (SR 14m for rehabilitation); Bilal Mosque in Los Angeles; repairs of the Rock Tomb and Omer bin al Khattab Mosque in al Quds; and Central Brent Mosque in Britain. King Fahd also established a number of scholarships and academic chairs in foreign prominent universities and colleges.

We can cite King Abdul Aziz Chair for Islamic Studies at the University of California, King Fahd Chair for Islamic Sharia Studies at the College of Law at Harvard University, King Fahd Chair for Studies at the Oriental and African Studies Institute at the University of London, and Prince Naif Department for Islamic Studies at the University of Moscow.

The Kingdom also established a number of Islamic academies abroad. Among them are the Islamic Academy in Washington at a cost of 100 million US dollars, where multinational students are taking lessons. Now it accommodates 1,200 students, of which 549 are Saudis. The rest represent 29 nationalities; King Fahd Academy in London whose students belong to 40 nationalities; King Fahd Academy in Moscow; King Fahd Academy in Bonn, which cost 30

million German Marks. A number of institutes, designed to spread Islamic culture and the Arabic language were also opened in foreign countries to serve Islamic communities in non-Muslim countries. They include the Arab Islamic Institute in Tokyo, an affiliate of the Riyadh-based Imam Mohammed bin Saud Islamic University.

Moreover, there are several Islamic schools (e.g. in South Korea) where 20,000 Muslims have formed the Korea Islamic Federation. King Fahd has appropriated an annual donation worth 25,000 US dollars to the federation. There are also many Islamic institutes all over the world, most notably the Arab and Islamic Institutes in Washington, Indonesia, Ras al Khaimah Emirate (UAE), Nouakchott (Mauritania), and Djibouti. The Institute of the History of Arab and Islamic Sciences in Frankfurt, Germany, receives an annual financial support from the Kingdom worth 15 million German Marks while the Arab World Institute in Paris receives considerable Saudi contribution to its annual budget.

110

A COMPARATIVE ASSESSMENT OF SAUDI ARABIA WITH OTHER COUNTRIES OF THE ISLAMIC WORLD

Targeting Terrorist Finances Project*
Watson Institute for International Studies
Brown University

June 2004

During the December 2003 discussion by the Task Force of the Columbia University team's assessment of Saudi Arabia, Task Force members commented on the importance of assessing the extent of Saudi Arabia's compliance with international standards in comparison with other states. In particular, given similarities in legal, administrative, and governmental structures, it would be important to consider measures taken in other countries of the Islamic world. This is especially true with regard to the regulation of charities and informal value transfer systems. Countries located in the Islamic world are also more likely to be sources of potential funds raised or locations for the transmission of funds to groups like al-Qaeda.

Over the past two and a half years, a research team at Brown University's Watson Institute for International Studies has been investigating the extent to which countries across the globe have been complying with and implementing international standards to counter the financing of terrorism. The Targeting Terrorist Finances Project, represented on the Task Force by Thomas Biersteker, is investigating degrees of compliance and implementation of the counter-terrorism effort by examining publicly available reports

* Members include Thomas J. Biersteker and Sue Eckert, Project Co-Directors, Peter Romaniuk, Graduate Research Assistant, and Jesse Finkelstein, Elizabeth Goodfriend, and Aaron Halegua, Undergraduate Research Assistants.

from different countries, along with other sources of country-specific information. Countries are evaluated relative to each other according to their degree of compliance of mandatory provisions of resolutions passed by the UN Security Council and other relevant indicators (particularly those recommended by the Financial Action Task Force (FATF)).

The research team has built on its previous work on the implementation of targeted financial sanctions,[1] differentiating between four aspects of policy implementation: (1) the establishment of a legal framework; (2) the creation or strengthening of an administrative infrastructure; (3) the introduction and use of a variety of different regulatory measures; and (4) evidence of enforcement. At the request of the Council Task Force co-directors, the Watson Institute project team has undertaken a systematic analysis of Saudi compliance in comparison to that of other countries of the Islamic world. The project has compared Saudi Arabia with nine other countries: Egypt, Indonesia, Jordan, Malaysia, Morocco, Pakistan, Tunisia, the United Arab Emirates, and Yemen. This is not a comprehensive sample, but it is representative of major regional financial centers, countries centrally involved in the global counter-terrorist effort, countries exhibiting a variety of different approaches and degrees of policy innovation, and different regions of the Islamic world (from North Africa to Southeast Asia).

The Watson Institute team has relied on publicly available documents submitted to the United Nations' Counter Terrorism Committee (responsible for implementing Security Council resolution 1373, criminalizing the provision of funds to groups utilizing terrorism) and the United Nations' 1267 Committee (responsible for targeted sanctions

against the Taliban, members of al-Qaeda, and associated entities). While these reports consist largely of self-reporting by states, they also include queries by issue area experts and state responses to those queries. This is an iterated process, with most states supplying two or three successive reports. In addition, the research team has drawn upon 1267 Committee monitoring group reports, conversations with individuals involved in the UN monitoring and assistance effort, reports of the joint IMF/World Bank assessments of country compliance with anti-terrorism measures, information provided directly by governments, newspaper and other media sources, and the research on Saudi Arabia carried out by students at Columbia University. The evaluation that follows is not based on in-country field research work or interviews conducted by members of the Watson Institute research team.

The assessment provided below should be read as a provisional one. There is not fully comparable information available on all of the countries. Moreover, this is a dynamic and constantly changing process, and accordingly, the Watson Institute research team welcomes corrections, additions, or clarifications regarding the countries included in the comparative assessment.

Method of Analysis

For the purposes of systematic comparison, each of the ten countries has been evaluated according to the following criteria.

---

[1] *Targeted Financial Sanctions: A Manual for Design and Implementation, Contributions from the Interlaken Process* (Published by the Swiss Confederation in cooperation with the UN Secretariat and the Watson Institute for International Studies, Brown University, 2001).

Legal Framework

With regard to the establishment of an adequate legal framework, states were accorded the highest evaluation if they have legislation in place that criminalizes the provision of funds for terrorism, have the ability to act to freeze funds immediately, and have signed the International Convention for the Suppression of the Financing of Terrorism. Each of the three criteria is defined more precisely below.

1. **Criminalization of Terrorist Financing**: States have criminalized the raising or provision of funds for terrorist acts, whether or not an act has been committed.
2. **Capacity to Freeze**: States have the authority to freeze funds expeditiously without prior judicial action (wherever that authority resides).
3. **Terrorist Financing Convention**: States have signed (or ratified) the International Convention for the Suppression of the Financing of Terrorism.

Administrative Infrastructure

With regard to the creation or strengthening of their administrative infrastructure to address terrorist financing, states were accorded the highest evaluation if they have a Financial Intelligence Unit, have committed additional resources to strengthen their institutional capacity, and have requested or received assistance for strengthening their administrative infrastructure from another state, or from an international or regional organization. Each criterion is defined more precisely below.

1. **FIU**: Countries have in place an established Financial Intelligence Unit.
2. **Additional Resources**: There is evidence of an increase in personnel or funds for building the institutional capacity to deal with some aspect of terrorist financing.

3. **Requested/Received Assistance**: The country has requested or received assistance related to financial law and practice, training for financial institutions, etc.

Regulatory Measures

With regard to the introduction and use of a variety of different regulatory measures, states were accorded the highest evaluation if they have gone beyond the United Nations' list of individuals or groups associated with the use of terrorism, if they have introduced measures to ensure bank and financial institution compliance, have established systems for regulating or registering informal value transfer systems (IVTS or *hawalas*), and if they have taken steps to regulate and monitor the operations of charities within and beyond the borders of their country. Each criterion is defined more precisely below.

1. **Listing**: Countries showed evidence of implementing lists that go beyond that promulgated by the UN (i.e. either their own list or the US Treasury's OFAC list).
2. **Bank/FI Compliance**: Countries have introduced at least three of the following measures:
    (a) Banks were notified of the names of individuals or groups.
    (b) Reporting requirements have been placed on banks.
    (c) Reporting requirements have been extended to other financial institutions beyond banks.
    (d) There is evidence that assistance was provided to banks.
3. **IVTS**: Countries have established some system for registering or regulating Informal Value Transfer Systems (*hawalas*).

4. **Charities**: Countries regulate and monitor the operations of charities within (and beyond) their borders.

Enforcement

With regard to enforcement, states were accorded the highest evaluation if they have actually frozen funds, made arrests or pursued prosecutions related to the financing of terrorism, and if there was other significant evidence of enforcement related to the financing of terrorism. Each criterion is defined more precisely below.

1. **Freezing of funds**: Countries have frozen terrorist assets, either pre-9/11 (under United Nations Security Council Resolution S/RES/1267) or subsequently. Most of this information was derived from Appendix III to S/2003/1070, published by the United Nations.
2. **Arrests since 9/11**: Countries have made arrests relating to the financing of terrorism.
3. **Other evidence**: There is some tangible evidence of additional enforcement, such as countries like Saudi Arabia that have bilateral cooperation arrangements with the United States specifically related to terrorist financing.

This framework enables the project team to evaluate degrees of compliance with mandatory provisions of resolutions passed by the UN Security Council and other relevant (FATF) indicators. For present purposes, the team deployed this framework to derive comparative assessments. In doing so, each country was initially evaluated independently by two different members of the project team. After their initial, independent evaluations, the two met to determine a consensus assessment, based on their

best interpretation of the information available about the country involved (and in an explicit effort to establish consistent evaluation and inter-coder reliability standards). Each country was evaluated based on the most recently available assessments (usually dating from 2003 and 2004) on each of the criteria listed above. We state our findings below in terms relative degrees of compliance and implementation, i.e. states that have complied with or implemented all or the vast majority of the measures elaborated in the numbered paragraphs above, are judged to be relatively "stronger" than those that have complied with or implemented fewer or none at all, who are therefore considered to be relatively "weaker."

Findings

Assessed according to the framework set out above, Saudi Arabia appears relatively compliant with standards to suppress the financing of terrorism when viewed in relation to other states from the Islamic world. While in some areas, most notably in regulatory measures, Saudi Arabia does not achieve as high a degree of compliance as others in the sample, in other aspects, particularly the establishment of a legal framework, Saudi Arabia's effort equals or exceeds measures taken by others. The comparative assessment is summarized in the table below.

Relative Degrees of Compliance and Implementation

← STRONGEST			WEAKEST →
Legal Framework	Indonesia Morocco Saudi Arabia Tunisia	Jordan Malaysia Pakistan	Egypt UAE Yemen
Administrative Infrastructure		Egypt Indonesia Malaysia	Jordan Pakistan Tunisia

		Morocco Saudi Arabia UAE Yemen		
Regulatory Measures	UAE Yemen	Egypt Malaysia Saudi Arabia	Indonesia Jordan Pakistan Tunisia	Morocco
Enforcement		Pakistan Saudi Arabia UAE	Indonesia Morocco Yemen	Egypt Jordan Malaysia Tunisia

Each of the rows in the table corresponds to elements of the analytical framework presented previously (legal, administrative, regulatory, and enforcement). Within each row, states that achieve full compliance with all of the criteria are rated "strongest," and states that are abjectly non-compliant on all measures are rated "weakest." Empty cells reflect instances in which none of the states in the sample was coded as fully compliant or abjectly non-compliant.

Following the recent assessment of Saudi Arabia's compliance with FATF standards, the financial press reported that the country has "world class" terrorist financing laws.[2] From the comparative evaluation summarized above, Saudi Arabia's legal framework appears to be among the more robust of the sample. For example, in Saudi Arabia, "terrorist financing" (that is, the collection and movement of funds intended for terrorism, whether or not a terrorist act actually occurs) is now criminalized. Other states have not created a separate offense for terrorist financing, contrary to FATF standards. A number of states in the comparative study (such as Yemen) have taken the

[2] Robin Allen, "Saudis meet anti-terrorist financing benchmarks: International assessment," *Financial Times*, 8 March 2004, p. 7.

step of listing terrorist financing as a predicate offense pursuant to anti-money laundering legislation. While this is an important step, it is not sufficient in itself, as it requires that a terrorist act occur before its financiers can be charged. Regarding the timing of legislative change in Saudi Arabia, the introduction of these and other measures reflect a sense of urgency induced by the May 2003 and subsequent bombings. Other states that have experienced devastating attacks on their territory (such as Indonesia) also criminalized terrorist financing subsequent to such violence.

In other ways, too, Saudi Arabia's legal framework compares favorably against other states in the sample. Saudi authorities now possess the legal power to freeze suspected terrorist assets expeditiously. Other states (such as Egypt) still require that separate judicial authority be sought prior to each freezing action. And again, others have not acted as quickly as the Saudis in ensuring capacity to freeze.

Finally, as a signatory to the UN Convention for the Suppression of the Financing of Terrorism, Saudi Arabia has taken on binding commitments to combat terrorist financing. While Saudi Arabia is yet to ratify the Convention, nearly half of the states in the sample have not yet signaled their willingness to act against terrorism in this way (e.g. Malaysia, Pakistan, the UAE, and Yemen are still debating whether or not to sign). In sum, Saudi Arabia's effort to establish a legal framework to suppress terrorist financing is relatively strong, and among the strongest of the states surveyed. However, as the Task Force report notes, "The passage of laws and regulations is only the first step toward the creation of an effective anti-money laundering and counter-terrorist financing regime. Just as important – and more important over the longer term – is effective implementation."

Saudi Arabia compares less favorably when its administrative infrastructure to support the implementation of terrorist financing measures is examined. In developing the capacity to act against terrorist financing effectively, states are expected to create a Financial Intelligence Unit. Saudi Arabia's recent initiatives in this regard fulfill this requirement, where others in the sample (such as Jordan and Pakistan, where legislation establishing an FIU remains in process) have not. However, there is no publicly available evidence that Saudi Arabia has committed additional resources to combat terrorist financing. While at least one other state (Morocco) has increased personnel for building the institutional capacity to deal with aspects of terrorist financing, there is no clear evidence that Saudi Arabia has committed additional resources to the counter-terrorist financing effort. Lastly, along with most other states in the sample, Saudi Arabia has utilized multilateral mechanisms and requested assistance for capacity-building needs to implement new legislative mandates. Seven out of the ten states surveyed have requested assistance in developing financial law and practice.

Regarding regulatory measures, when viewed in comparative perspective, Saudi Arabia performs well, but not outstandingly. Saudi Arabia has utilized the UN Security Council list of individuals and entities belonging to, or associated with, Osama bin Laden, al Qaeda, and the Taliban. It had even taken action against some of those listed prior to the passage of UN Security Council Resolution 1267, by freezing the accounts of Osama bin Laden in 1994. Other countries included in the comparative assessment (such as the United Arab Emirates and Pakistan), however, have implemented more extensive lists, including the list developed by the US Treasury's Office of Foreign Asset Control.

Overall, Saudi Arabia has made relatively strong progress in ensuring that the formal banking sector complies with new measures to combat terrorist financing. It is only one of three countries (the others are Egypt and Malaysia) that have taken steps to notify domestic banks of their obligations in this regard, to impose reporting requirements on banks, to extend these requirements to non-bank financial institutions, and to provide assistance to banks and financial institutions in implementing new legal and administrative measures. This record of activities compares favorably with Morocco and Pakistan (which have not enhanced reporting requirements) and Indonesia, Tunisia, the UAE and Yemen (which have not yet undertaken activities to assist compliance by banks and other financial institutions).

Similar to other states included in the comparative evaluation, Saudi Arabia initially denied the existence and prevalence of informal value transfer systems (IVTS), and declared them illegal under non-specific legal mandates (e.g. Sharia Law). Saudi Arabia has since taken specific measures to bring *hawaladars* into the broader regulatory framework. In doing so, it has followed the lead of the UAE, which has shown initiative in developing and implementing measures to improve the accountability of IVTS mechanisms (e.g. by imposing registration, reporting and record-keeping requirements upon IVTS operators). These recent initiatives distinguish Saudi Arabia from other states that continue to deny the existence of IVTS in their country (such as Morocco and Tunisia), or have not yet acted to impose basic transparency requirements on *hawaladars* (e.g. Jordan).

If Saudi Arabia was slow to act against IVTS, however, it has been among the first and most stringent in regulating charities operating in the non-profit sector. Saudi

charities are now among the best regulated in the sample (these measures are outlined in the main body of the Task Force report). Other states have improved their legislative and administrative responses to terrorist financing without extending measures to the non-profit sector (e.g. Indonesia), or have yet to impose transparency requirements upon charities (e.g. Pakistan).

Of the ten countries surveyed, Saudi Arabia has one of the relatively stronger records of enforcing the measures it has taken to combat terrorist financing. Of course, the fact that Saudi Arabia is relatively wealthier and has historically been reputedly one of the largest sources of financial support for groups utilizing terrorism, suggest that it should be able to demonstrate relatively more evidence of enforcement than most of the other countries included in the comparative assessment. A more robust conclusion would require that Saudi Arabia be compared with countries that present a comparable risk in terms of the raising and movement of terrorist funds. Within this limitation, Saudi Arabia is reported to have frozen the second largest amount of terrorist-related assets of the countries included in the sample (after Pakistan).[3] In at least one instance, however, funds were allegedly frozen and then returned to the depositor.[4] Nevertheless, because the Saudi government has reported that it has closed a total of forty-one accounts, it has therefore been credited in this comparative assessment with showing evidence of enforcement.

The Saudi government claims to have made arrests related to terrorism, but from a review of publicly available sources, there is no evidence that any arrests have been made

[3]Appendix III to S/2003/1070, published by the United Nations. Saudi Arabia has reportedly frozen $5.7m, compared with Pakistan's $10.7m.

specifically related to terrorist financing. Finally, the fact that Saudi Arabia is involved in a bilateral initiative with the United States to enforce measures against terrorist financing suggests tangible evidence of additional enforcement.

This comparative assessment of Saudi Arabia is based entirely on public source documents and has not benefited from interviews with any of the principals involved in the bilateral initiative. Thus, the conclusion that Saudi Arabia shows certain evidence of enforcement should not be interpreted as a contradiction of the Task Force conclusion regarding the nature of Saudi enforcement. However, this comparative study shows that few states are able to produce compelling evidence of enforcement. Viewed in this perspective, Saudi Arabia enforces counter-terrorist financing measures relatively strongly and is grouped with those countries showing the greatest evidence of enforcement.

Conclusions

While the results of this research are provisional, within the context of a systematic comparative analysis of legal frameworks, administrative infrastructure, regulatory measures, and enforcement across ten countries of the Islamic world, Saudi compliance with counter-terrorist financing measures is relatively strong. There are certainly additional measures it can take in each of these areas. It could ratify the terrorist financing convention, devote additional resources to its administrative infrastructure, register and monitor IVTS, and make public arrests related to terrorist financing.

---

[4] Douglas Farah, "U.S. – Saudi Anti-Terror Operation Plan: Task Force Will Target Funding, Washington Post, August 26, 2003, p. A1.

These findings underscore the importance of ongoing international engagement on the issue of terrorist financing. Across the world, states have initiated legislative and administrative changes in response to the need to suppress terrorist financing. Exemplifying this broad trend, Saudi Arabia has responded to external criticism of its compliance with international standards to suppress terrorist financing. In doing so, it has achieved a relatively strong degree of compliance in comparison with other states in this sample of states from the Islamic world; but clearly, more needs to be done to improve and verify compliance and implementation across all states. This points to the general need for ongoing and appreciably enhanced international coordination, monitoring, assessment, and capacity building efforts, as discussed in Recommendation 3 of the Task Force report.

A TECHNICAL ASSESSMENT OF CERTAIN SAUDI ARABIA LAWS, REGULATIONS, AND INSTITUTIONS

Excerpts of a December 2003 review of the new Saudi Arabian legal, regulatory, and institutional regime to combat money laundering and terrorist financing, commissioned by, and presented to, the Independent Task Force on Terrorist Financing sponsored by the Council on Foreign Relations.

Methodology

The report's analysis is divided into three chapters: Criminal Law, Regulatory Regime, and International Cooperation. The Criminal Law chapter assesses the criminalization of money laundering and terrorist financing in Saudi Arabia, and the agencies charged with enforcing these provisions. The Regulatory Regime evaluates the regulatory framework in Saudi Arabia as applicable to the financial, commercial and non-profit sectors, with a brief overview of the "informal" sector. Finally, the International Cooperation chapter addresses the mechanisms and procedures that Saudi Arabia has put in place for coordination of its anti-money laundering and combating terrorist financing (AML/CTF) efforts with those of other jurisdictions.

Each chapter contains sub-chapters, which represent independent themes within that chapter. For example, the Criminal Law chapter is divided into Scope of Money Laundering Offense, Scope of Terrorist Financing Offense, Sanctions, Designation of Authorities, and Capacity of Authorities. Each sub-chapter, is divided into a number of principles relevant to assessing Saudi Arabia's compliance with international standards and relating to that sub-chapter's theme. For example, the Sanctions sub-chapter within Criminal Law chapter contains the principle - Confiscating and Attaching Terrorist Assets.

Many, though not all of these principles are drawn from the Financial Action Task Force's "40 Recommendations on Money Laundering" and its "8 Special Recommendations on Terrorist Financing."

For each principle, we assessed Saudi Arabia's compliance from a legal perspective, an enforcement perspective, and an implementation perspective. The legal perspective examined the relevant Saudi laws and regulations, and evaluated their soundness and thoroughness. The enforcement perspective examined the governmental authorities charged with enforcing these laws and regulations, and evaluated their enforcement activity. The implementation perspective examined the persons and entities subject to the laws and regulations, and evaluated the impact on their conduct. Not all perspectives are relevant to each principle.

The documentary evidence we compiled included both primary sources, consisting of Saudi laws and regulations, and secondary sources, such as Congressional testimony, treatises by legal scholars, and news reports. In addition, we interviewed various persons with relevant banking, legal or other expertise.

As part of our effort to conduct a professional-caliber analysis of the laws, regulations, institutions and practices of Saudi Arabia, in early October we sent a detailed request for information and documents on these topics to the Saudi Arabian Foreign Policy Advisor, Mr. Adel Al-Jubeir. Unfortunately, we did not receive any documents or information in response to this request.

Wherever applicable, we based our analysis of Saudi Arabia's AML/CTF efforts on relevant international standards, in accordance with the FATF Recommendations. These standards included:

- 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances ("The Vienna Convention")
- 1999 International Convention for the Suppression of the Financing of Terrorism
- 2000 United Nations Convention Against Transnational Organized Crime ("The Palermo Convention")
- 2001 UN Security Council Resolution 1373
- 1999 Basel Committee on Banking Supervision Core Principles and Methodology ("The Basel Principles")
- 2002 FATF Best Practices Guidelines on Combating the Abuse of Non-Profit Organization (The "FATF NPO Guidelines")

- Egmont Group Financial Intelligence Unit Definition
- Corporate best practices from leading financial institutions
- Basel Customer Due Diligence Guidelines

Criminal Law

A vital component of a country's anti-money laundering and combating terrorist financing (AML/CTF) effort is its criminalization of the core conduct of money laundering and terrorist financing. Such criminalization brings to bear the investigative resources of the criminal law enforcement authorities, as well as the deterrence effect of criminal sanctions. In addition, the thoroughness with which a country criminalizes ML/FT activity sends an important public message about its determination to eradicate such activity, while stigmatizing and delegitimizing those who engage in it.

This chapter will examine the criminal law component of Saudi Arabia's AML/CTF effort along five vectors:

- Scope of Money Laundering Offense: The adequacy of the legal scope of money laundering as a criminal offense, including the definition of money laundering, the associated mental state requirement, and the extension of money laundering criminal liability to legal persons.
- Scope of Terrorist Financing Offense: The adequacy of the legal scope of terrorist financing as a criminal offense, including the definition of terrorist financing, the associated mental state requirement, and the extension of terrorist financing criminal liability to legal persons.
- Sanctions: The adequacy of criminal sanctions against natural or legal persons that engage in money laundering or terrorist financing, including both pre-trial attachment of suspect assets and post-conviction imprisonment, confiscation and other criminal penalties.
- Designation of Authorities: The adequacy of the formal designation and legal empowerment of law enforcement authorities charged with enforcing the criminal law AML/CTF provisions, including their authority to demand and obtain evidence and information.
- Capacity of Authorities: The adequacy of the law enforcement authorities' capacity to carry out their mandate, including their human and financial resources, their level of coordination, and the systems of information tracking at their disposal.

Scope of Money Laundering Offense

Compliance with international AML/CFT standards entails a thorough legal definition of the scope of a country's money laundering offense. Money laundering comprises a variety of activities, relating both to the predicate offenses that generated the "dirty" funds and to the transfer, concealment, possession and use of such funds. If a country does not adequately define money laundering, loopholes may exist that could enable or permit illegal money laundering activities.

Special care needs to be devoted to the issue of the mental state to be associated with the crime of money laundering. The criminal act of money laundering can encompass a variety of actors, having different levels of culpability and playing different roles in the money laundering process. If a country does not adequately address the mental state requirement, persons or legal entities who contribute to a money laundering offense may improperly escape criminal liability for their actions. To this end, countries must also permit mental state to be inferred from objective factual circumstances.

Finally, the scope of a country's money laundering offense ought to address the issue of legal person liability. If legal persons, such as corporations or associations, are not covered by a country's definition of a money laundering offense, these entities may be able to conduct money laundering activities without facing law enforcement authority sanctions – and thus serve as a "safe conduit" of laundered funds.

Principle 1: Definitional Scope of Criminal Offense of Money Laundering

Standard:

In accordance with FATF Recommendation 1[21], we have used the 2000 United Nations Convention against Transnational Organized Crime (the "Palermo Convention") and the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the "Vienna Convention") for guidance in assessing Saudi Arabia's compliance with this principle[22]. Specifically, in assessing the definitional scope of the criminal offense of money laundering, we have looked to the language in Articles 2 and 6 of the Palermo Convention, and Articles 1 and 3 of the Vienna Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be substantially in compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

In August 2003, Saudi Arabia enacted the Anti-Money Laundering Law (the "KSA-AMLL")[23]. The core definition of the criminal offense of money laundering is set forth in Article 2 of the KSA-AMLL, with certain aggravating circumstances singled out for more severe sanction in Article 17. Relevant terms are defined in Article 1.

We have found Saudi Arabia to be substantially in compliance with this principle from a legal perspective.

The definition of money laundering in Article 2 of the KSA-AMLL appears to be at least as broad as the corresponding language in the Palermo and Vienna Conventions. The aggravating circumstances in Article 17 of the KSA-AMLL closely track the language in Article 3(5) of the Vienna Convention.

The reason we do not consider Saudi Arabia fully compliant with this principle centers on the term definitions in Article 1 of the KSA-AMLL, which are not as rigorously drafted as the corresponding definitions in the Palermo and Vienna Conventions.

a. *Proceeds.*

The term "proceeds" as defined in KSA-AMLL Article 1(3) "shall mean any *funds* generated or earned directly or indirectly *from money-laundering offences* subject to sanctions hereunder" (emphasis added). In the Palermo Convention, Article 2(e) defines "proceeds of crime" as "any

[21] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.
[22] The full text of both Conventions is appended to this report in Annex 1.
[23] The full text of the law is appended to this report in Annex 1.

property derived from or obtained, directly or indirectly, *through the commission of an offence*." Therefore, (1) the Saudi definition excludes from the definition of "proceeds" any property derived from the commission of offenses other than money laundering offenses, and (2) the Saudi definition excludes any property other than funds.

a.1. *Property derived from non-money laundering offenses.*

The first exclusion does not effect a significant loophole because of the way the KSA-AMLL defines a money laundering offense. However, it does lead to unnecessary ambiguity regarding the relationship that prosecuting authorities would have to prove between the property in question and the offense to which it is connected.

Whereas the Palermo Convention instructs States Parties to criminalize "[t]he conversion or transfer of property, knowing that such property is the proceeds of crime," the corresponding KSA-AMLL language is "[c]onducting any transaction involving property or proceeds with the knowledge that such property or proceeds came as a result of a criminal activity or from an illegal or illegitimate source." This definition's reference to "property or proceeds [derived from] an illegal . . . source" is somewhat awkward, in that the definition of the term "proceeds" appears to have already incorporated a connection to an illegal source. Nonetheless, the redundancy ensures that any property derived from any crime, including a non-money laundering crime, is covered by its provisions.

However, the Saudi language fails to clarify that the definition of a money laundering offense applies to transacting in property derived *directly or indirectly* from a non-money laundering crime. The definition of "proceeds" in Article 1 does spell out that proceeds can be earned or generated "directly or indirectly" from an offense – but it only covers money laundering offenses. The language in Article 2, regarding "property [that] came as a result of a criminal activity," is useful in that it covers all crimes, but it does not make clear that "came as a result" includes indirect as well as direct derivation. Thus, it is arguable that for property derived from offenses other than money laundering offenses, the prosecuting authorities may have to prove that the property was derived *directly* from the crime – a higher burden than the one mandated by the Palermo Convention.

a.2. *Property other than funds.*

The second exclusion does not effect a significant loophole for reasons similar to those discussed above – the redundancy in the Article 2 language, which refers to both property and proceeds, allows the broad definition of "property,"which includes all types of assets, to supplement the narrower definition of "proceeds," which excludes assets other than funds. However, this solution suffers from the same flaw – relying on the "property" language in Article 2 underscores the ambiguity regarding the requisite connection between "property" and the offense from which it is derived.

b. *Property.*

The term "property" as defined in KSA-AMLL Article 1(2) "shall mean any kind of assets and property, whether material or immaterial, movable or immovable, and legal documents and instruments which prove the ownership of the assets or any right attached thereto." Article 2(d) of the Palermo Convention defines "property" as "assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets." It is unclear whether the reference to "right attached

thereto" in the KSA-AMLL corresponds to the Palermo Convention's "interest in" the assets. It is arguable that the Saudi definition excludes documents and instruments evidencing an interest in assets.

Although we understand that Saudi property law does not recognize interests in property other than ownership[24], such an exclusion of interests in assets – e.g. leaseholds – from the definition of property would be improper. Money laundering is a transnational phenomenon, and the Saudi judiciary should be equipped to rule on cases involving interests in assets held in jurisdictions that recognize such interests, even if Saudi Arabia itself does not recognize them.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have been informed by official sources that the Saudi Ministry of Justice is conducting training for *shari'a* judges on money-laundering offenses.[25] However, we have no details on the content of such training; therefore, we cannot assess whether such training sufficiently ensures that the definitional scope of the money laundering offense is understood and implemented by the judiciary.

[24] Interview with a Saudi attorney, 12/13/03. We understand that interests in property other than ownership are given de facto recognition in Saudi courts. However, this recognition has not been formalized *de jure* to our knowledge, thus leaving open the question of the treatment of such interests in the KSA-AMLL.
[25] Interview, Senior U.S. Government official, 11/21/03

Principle 2a: Mental State Requirement of Criminal Offense of Money Laundering

Standard:

In accordance with FATF Recommendation 2(a)[26], we have used the Palermo Convention and the Vienna Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the mental state requirement of the criminal offense of money laundering, we have looked to the language in Article 6 of the Palermo Convention, and Article 3 of the Vienna Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The core definition of the criminal offense of money laundering, set forth in Article 2 of the KSA-AMLL, describes the mental state required by the offense.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective.

The mental element required by the KSA-AMLL definition of the criminal offense of money laundering is in line with the language of the Vienna and Palermo Conventions – namely, knowing that the property in question came as a result of criminal activity suffices to convict a defendant, even if such knowledge was not accompanied by an intent to assist the process of money laundering.

The reason we consider Saudi Arabia only partially compliant with this principle has to do with two main concerns.

First, Article 21 of the KSA-AMLL exempts from liability "those acting in good faith." Since Article 2 already incorporates a mental state requirement into the definition of the offense, the need for the language in Article 21 is unclear. To the extent that an interpreter of the law, such as a judge, chooses to give Article 21 any effect – i.e., to acknowledge a "good faith" defense beyond the one inherent in the mental state requirement – the KSA-AMLL's language defining the mental state element of a money laundering offense would be undermined.[27]

Second, we note that the KSA-AMLL makes no explicit provision for inferring mental state from objective factual circumstances. There is no language in it that corresponds to Article 6(2)(f) in the Palermo Convention, or Article 3(3) of the Vienna Convention. We also note that the treatment

[26] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.
[27] According to a Saudi attorney, whom we interviewed on 12/13/03, the impact of the "good faith" exculpatory clause is unlikely to be significant.

of evidence in *shari'a* is heavily focused on confessions and witnesses, rather than circumstantial evidence.[28]

Additionally, we note that the KSA-AMLL makes no reference to "willful blindness" or "conscious disregard" as being sufficient to satisfy the "knowledge" mental state requirement outlined in Article 2. The international standards we used in evaluating Saudi Arabia's compliance with this principle do not require that the jurisdiction expressly establish "willful blindness" or "conscious disregard" as meeting the mental state requirement; nonetheless, failure to do so raises the possibility of a serious loophole in the criminalization regime.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

[28] According to a Saudi attorney, whom we interviewed on 12/13/03, there are few limitations on judicial notice in the *shari'a* court system. Thus, in practice, a judge could choose to infer mental state from circumstantial evidence – however, the admissibility of such an inference is not provided for by law and would depend on the judge's personal amenability to this type of argument.

Principle 2b(1): Extension of Money Laundering Criminal Liability to Legal Persons

Standard:

We have used the Palermo Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the extension of liability to legal persons, we have looked to the language in Article 10 of the Palermo Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Articles 3-10 of the KSA-AMLL discuss "Financial and Non-Financial Institutions" ("Institutions") and their obligations and liabilities under the KSA-AMLL. Article 18 establishes penalties for natural persons who are members of Institutions and fail to comply with the obligations set forth in Articles 4-10 (mainly administrative obligations and reporting requirements). Article 19 establishes penalties for Institutions that violate Articles 2 and 3, which relate to the primary offenses of ML/FT.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective.

The penalty imposed on Institutions that commit ML/FT offenses – which occurs when "such offenses [are] committed in their name or to their account" (Article 3) – is "a fine ranging from SR 100,000 [US $26,667] up to the value of the property involved in the offence" (Article 19). This would appear to satisfy the FATF recommendation of effective, proportionate and dissuasive sanctions. Moreover, the administrative obligations in Articles 4-10, backed by a sanction of "a jail penalty up to 2 years or a fine up to SR 500,000 [US $133,333]" (Article 18), enhance law enforcement agencies' ability to discover and investigate offenses by legal persons. Such enhancement serves to increase the deterrent effect of the penalties for legal persons' violating the primary obligations of Articles 2-3.

The reason we consider Saudi Arabia only partially compliant with this principle is the limited reach of the defined term "Financial or Non-Financial Institution."

Article 1(5) of the KSA-AMLL defines the term as "any establishment in the kingdom engaged in any one or more financial, commercial or economic activity such as banks, money-exchangers, investment companies, insurance companies, commercial companies, establishments, professional firms or any other similar activities set forth in the Implementation Rules." This definition excludes legal entities that are not engaged in financial, commercial or economic

activities, such as charities, religious associations, educational institutions and other non-profit organizations.

Although Article 2 of the KSA-AMLL, criminalizing the core ML/FT conduct, applies by its terms to "anyone" – presumably including all legal entities – the terms of Article 19 suggest that legal entity-level penalties are only applied to Financial or Non-Financial Institutions. It is unclear whether the KSA-AMLL imposes any penalties at all on non-profit organizations at the legal entity level.

In light of the important role that such non-profit organizations play in a devout Moslem society, the failure to extend the KSA-AMLL's reach to this class of legal persons constitutes a severe curtailment of the law's effectiveness in combatting ML/FT offenses.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have not been able to obtain data on enforcement of the KSA-AMLL's money laundering provisions against any legal entities. We have not been able to obtain data on the extent or nature of criminal law enforcement agencies' investigation and prosecution efforts against any legal entities.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have not been able to ascertain whether all types of legal entities in Saudi Arabia – financial institutions, commercial institutions, social and non-profit institutions – regard themselves as being covered by the KSA-AMLL's money laundering provisions.

Scope of Terrorist Financing Offense

Compliance with international AML/CFT standards entails a thorough legal definition of the scope of a country's terrorist financing offense. This requires an adequate definition of both the predicate offense of terrorism, and of the conduct that constitutes the financing thereof. If either of those are not sufficiently addressed by a country's criminal law regime, certain avenues of terrorist financing will remain legally available to offenders.

In addition, the same attention to mental state requirements and legal person liability is necessary in the terrorist financing context as in the money laundering context; failure to address these issues leads to analogous consequences.

Principle 42: Definitional Scope of Criminal Offense of Terrorist Financing

Standard:

We have used the UN CFT Convention and the UNSC R1373 for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be non-compliant with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Saudi Arabia signed the UN CFT Convention in November 2001, and has not ratified it[29]. UNSC R1373, adopted under Chapter VII of the UN Charter, is automatically mandatory on Saudi Arabia with no further action necessary on the kingdom's part. The offense of terrorist financing is set forth in the KSA-AMLL in Article 2(d).

We have found Saudi Arabia to be non-compliant with this principle from a legal perspective.

Article 2(d) of the KSA-AMLL provides that anyone who engages in "[f]inancing terrorism, terrorist acts and terrorist organizations" shall be deemed a perpetrator of a money laundering offense, subject to the sanctions associated with that offense.

We consider Saudi Arabia non-compliant with this principle for a number of reasons.

a. *Definition of Terrorism.*

We have not found any Saudi legislative definition of the crime of terrorism, despite its obligation under UNSC R1373, Article 2(e), to ensure that "terrorist acts are established as serious criminal offences in domestic laws and regulations". We also note that Saudi Arabia is not a signatory to the UN CTB Convention[30], which provides an internationally accepted definition for terrorist bombings in its Article 2.

We are concerned over the possibility that Saudi Arabia's judicial construction of the definition of terrorism (as the predicate offense for terrorist financing) might exclude acts and organizations deemed terrorist in nature by international law. We note that the Arab Convention for the Suppression of Terrorism, and the Convention of the Organization of the Islamic Conference on Combating International Terrorism, to both of which Saudi Arabia is a signatory, define as a terrorist

---

[29] Information on signature and ratification status is based on documents provided on the United Nations' website, at <http://untreaty.un.org/ENGLISH/Status/Chapter_xviii/treaty11.asp> (last visited on Nov. 16, 2003).

[30] Information on signature and ratification status is based on documents provided on the United Nations' website, at <http://untreaty.un.org/ENGLISH/Status/Chapter_xviii/treaty9.asp> (last visited on Nov. 16, 2003).

crime and a terrorist offense, respectively, only acts of terrorism committed in the Contracting States or against their nationals, property or interests. Even should this definition be broadened by analogy to include acts committed against non-Contracting States, both treaties' definitions of terrorism exclude acts of armed struggle against foreign occupation. This exclusion would appear to cover, for example, acts by Chechen separatists against Russian civilians, acts by splinter IRA factions against British civilians, and acts by Palestinian rejectionist groups against Israeli civilians – all of which are recognized as terrorism by international law.

b. *Definition of Financing.*

The KSA-AMLL is insufficiently detailed with respect to its definition of terrorist financing. The UN CFT Convention, which is used as a benchmark by FATF, sets forth in Article 2(1) a more detailed and specific definition, including an intentional element (*mens rea*); its language reads, in relevant part,

> Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out [acts of terrorism].

UNSC R1373, also used as a benchmark by FATF, provides the following specific language in Article 1 as guidance:

> [A]ll States shall . . . [c]riminalize the wilful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts . . .
>
> [and p]rohibit their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit or facilitate or participate in the commission of terrorist acts, of entities owned or controlled, directly or indirectly, by such persons and of persons and entities acting on behalf of or at the direction of such persons.

We understand that laconic legal definitions are not uncommon in Saudi *nizams*, and that such definitions are later augmented by administrative regulations.[31] However, we have not seen any such regulations on the subject of terrorist finance, and we are concerned over the vagueness of the KSA-AMLL itself.

The conditioning of the financial assistance to the family upon the "martyrdom" of the suicide bomber would appear to meet the UNSC R1373 definition of terrorist financing, as an indirect benefit to the terrorist that alleviates his or her concerns for his or her family's financial security. However, it is doubtful whether such fund-collection would meet the KSA-AMLL definition of financing terrorism.[32]

c. *Mental State Requirement.*

---

[31] Interview with Professor Sherif Hassan of Columbia Law School.

[32] According to a Saudi attorney, whom we interviewed on 12/13/03, the KSA-AMLL almost certainly does not cover financial assistance to the Palestinian's armed struggle against Israel.

In contrast to the KSA-AMLL's definitions of money laundering offenses in Article 2(a)-(c), the definition of a terrorist finance offense in Article 2(d) does not specify a mental state requirement. Also, see analysis under Principle 2a.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 2b(2): Extension of Terrorist Financing Criminal Liability to Legal Persons

Standard:

We have used the Palermo Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the extension of liability to legal persons, we have looked to the language in Article 10 of the Palermo Convention.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Articles 3-10 of the KSA-AMLL discuss "Financial and Non-Financial Institutions" ("Institutions") and their obligations and liabilities under the KSA-AMLL. Article 18 establishes penalties for natural persons who are members of Institutions and fail to comply with the obligations set forth in Articles 4-10 (mainly administrative obligations and reporting requirements). Article 19 establishes penalties for Institutions that violate Articles 2 and 3, which relate to the primary offenses of ML/FT.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective. See analysis under Principle 2b(1).

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have not been able to obtain data on enforcement of the KSA-AMLL's terrorist financing provisions against any legal entities. We have not been able to obtain data on the extent or nature of criminal law enforcement agencies' investigation and prosecution efforts against any legal entities.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have not been able to ascertain whether all types of legal entities in Saudi Arabia – financial institutions, commercial institutions, social and non-profit institutions – regard themselves as being covered by the KSA-AMLL's terrorist financing provisions.

Sanctions

Compliance with international AML/CFT standards as regards a country's criminal law regime requires that effective and dissuasive sanctions be available to punish those who engage in

money laundering or terrorist financing conduct. Failure to provide, enforce or implement such sanctions will undermine the efficacy of any criminalization of ML/FT. In addition, appropriate authorities must have the ability to attach assets of persons involved in ML/FT offenses, to prevent their being transferred beyond the reach of the jurisdiction's enforcement arms.

Special care must be given to the definition of the assets subject to attachment or confiscation. For example, if a country distinguishes between assets directly involved in money laundering or terrorist financing and assets not directly involved, confiscatory sanctions may lose their power and deterrent effect, due to the ease with which some types of assets can be converted into others.

Principle 17a: Effective Criminal Sanctions

Standard:

We have used FATF Recommendation 17[33] for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be fully compliant with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Sanctions relevant to the AML/CFT criminal law in Saudi Arabia are provided in Articles 16-17 of the KSA-AMLL.

We have found Saudi Arabia to be fully compliant with this principle from a legal perspective.

Under the KSA-AMLL, a natural person found to be the perpetrator of a money laundering or terrorist financing offense is punishable by imprisonment of up to ten years and a fine of up to S.R. 5,000,000 (~ US $1,333,333) (Article 16); this penalty is increased to 15 years and S.R. 7,000,000 if certain aggravating factors are present (Article 17). In addition, property, proceeds and instrumentalities connected with the crime are subject to confiscation. See also analysis of regulatory sanctions and legal entity sanctions, under Principle 17b.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have been unable to determine whether law enforcement and prosecutorial agencies are seeking to take full advantage of the punitive range provided by the KSA-AMLL's sanctions provisions.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have been unable to assess the range of penalties meted by the *shari'a* courts for ML/FT offenses, and the extent of any deterrence engendered by such penalties.

---

[33] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

Principle 3: Confiscating and Attaching Money Laundering-Related Assets

Standard:

In accordance with FATF Recommendation 3[34], we have used the Palermo Convention and the Vienna Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing provisional measures and authority for confiscation, we have looked to the language in Article 12 of the Palermo Convention, and Article 5 of the Vienna Convention.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with the confiscation portion of this principle, and we have found Saudi Arabia to be substantially compliant with the attachment portion of this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL establishes a procedure for attaching assets in Article 12, and authorizes confiscation of assets in Article 16.

We have not been able to verify Saudi Arabia's compliance with the confiscation portion of this principle from a legal perspective. We have found Saudi Arabia to be substantially compliant with the attachment portion of this principle from a legal perspective.

a. *Confiscation.*

Article 16 of the KSA-AMLL subjects the "perpetrator of a money-laundering offence under Article (2) [to] the confiscation of the property, proceeds and instrumentalities connected with the crime. If such property and proceeds are combined with property generated from legitimate sources, such property shall be subject to confiscation pro rata with the estimated value of the illegitimate proceeds." The provision for pro rata confiscation of intermingled assets corresponds to Article 12(4) of the Palermo Convention and Article 5(6)(b) of the Vienna Convention.

We do not consider the Article 16 grant of confiscatory authority to be sufficient evidence of compliance with this principle for the following reasons:

a.1. *Conversion.*

Article 12(3) of the Palermo Convention and Article 5(6)(a) of the Vienna Convention require States Parties to ensure that, if proceeds of crime are transformed or converted into other property, such other property shall be liable to confiscation instead of the proceeds. The KSA-AMLL contains no such provision. Due to the ease with which some types of assets can be

[34] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

converted into others, this omission in the KSA-AMLL could severely undermine the reach of its confiscatory sanctions, unless addressed elsewhere in the Saudi legal system through provisions we have not seen.

a.2. *Income and benefits.*

Article 12(5) of the Palermo Convention and Article 5(6)(c) of the Vienna Convention require States Parties to ensure that income or other benefits derived from proceeds of crime – or property into which proceeds of crime have been converted – is subject to confiscation. The KSA-AMLL contains no such provision.

a.3. *Alternative property.*

Article 12(1)(a) of the Palermo Convention and Article 5(1)(a) of the Vienna Convention require States Parties to adopt measures to enable confiscation of property "the value of which corresponds to" that of proceeds of crime. This enables the State Party to deal with situations in which the proceeds of crime are not amenable to confiscation, by confiscating instead other property of equal value. The KSA-AMLL contains no such provision. Indeed, we are given to understand that *shari'a* does not permit the confiscation of any property other than the specific property that was implicated in the wrongful act in question.[35]

b. *Attachment.*

Article 12 of the KSA-AMLL authorizes the Financial Intelligence Unit (the "FIU") to direct government authorities "to attach properties, proceeds and instrumentalities committed in money laundering for a period not exceeding 20 days. If further extension is needed, the order must come from the competent court." This language provides the FIU with the necessary authority to cause assets to be frozen, and thus prevent them from being transferred or concealed, while proceedings meant to determine whether the assets should be confiscated take their course.

The reason we do not consider the Article 12 grant of attachment authority fully compliant with this principle is the brevity of the authorized attachment order. We are concerned that 20 days might not be sufficient for obtaining the requisite "order . . . from the competent court", especially during Ramadan or in summertime, when the pace of judicial proceedings in Saudi Arabia slows measurably[36]. Nonetheless, under most circumstances this period of time should be adequate, and therefore we consider the Article 12 language substantially compliant.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

---

[35] Interview with a Saudi attorney, 12/13/03.
[36] Interview with a Saudi attorney, 11/11/03.

Principle 43: Confiscating and Attaching Terrorist Assets

Standard:

In accordance with FATF Special Recommendation 3[37], we have used the UN CFT Convention and the UNSC R1373 for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be non-compliant with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL's confiscation and attachment provisions, discussed under Principle 3, provide the authority for confiscating and attaching terrorist assets.

We have found Saudi Arabia to be non-compliant with this principle from a legal perspective. In addition to the issues outlined in Principle 3 regarding the efficacy of the KSA-AMLL confiscation and attachment provisions in general, the following additional concerns relate to those provisions as applied to terrorist finance offenses:

a. *Assets of terrorists and terrorist organizations.*

Article 1(c) of UNSC R1373 calls upon States to

> [f]reeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities . . .

The language quoted above clearly instructs States to freeze assets of terrorists and terrorist organizations, without limiting its reach solely to those assets that have actually been committed to the financing of terrorism. By contrast, the attachment provisions in Article 12 of the KSA-AMLL, and the confiscation provisions in Article 16, limit themselves to "properties, proceeds and instrumentalities" that are connected to the crime.

b. *Pro rata confiscation of intermingled funds.*

[37] The full text of the FATF 8 Special Recommendations on Terrorist Financing is appended to this report in Annex 2.

Article 16 of the KSA-AMLL states that if "property and proceeds [connected with the crime] are combined with property generated from legitimate sources, such property shall be subject to confiscation pro rata with the estimated value of the illegitimate proceeds." The wording of this provision appears to place a considerable segment of terrorist financing assets beyond the reach of the KSA-AMLL's confiscatory power.

"Proceeds" are defined in Article 1(3) as funds generated from money laundering offenses (including terrorist finance offenses). This definition does not cover assets that are intended for use in terrorist acts, if they are not originally derived from a criminal activity. Therefore, in the case of intermingled assets that include property intended for use in terrorist acts as well as other property, "the estimated value of the illegitimate proceeds" will be nil, and the pro rata confiscation will perforce be limited to nil – as long as the terrorist financing assets themselves are not derived from a criminal activity.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Designation of Authorities

Compliance with international AML/CFT standards requires appropriate formal designation and legal empowerment of law enforcement agencies. If a country does not designate such authorities to assume responsibility for AML/CFT enforcement, significant obstacles may exist with regards to the efficient monitoring of money laundering and terrorism financing, as well as to the appropriate reporting of these crimes. Lack of clarity in the designation can lead to confusion among law abiding citizens, such as employees of a financial institution or any other business, regarding their legal obligation to report a suspicious transaction or the appropriate method of reporting money laundering and terrorism financing offenses. Other obstacles may arise if several competing government organizations claim the right to enforce the law, as well as monitor, report and prosecute money laundering and terrorism financing offenses.

In addition to the problems inherent in a faulty formal designation of appropriate authorities, the designated authorities will face further problems and obstacles to enforcing the law unless they have the appropriate legal empowerment. In particular, they must have the authority to obtain pertinent documents and information from persons and institutions. Without such legal authority, enforcement agencies will be severely hampered in carrying out their mandate.

Principle 27: Designation of Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 27[38] for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL designates authorities to enforce its criminal provisions and assist in AML-CFT investigations. Article 27 of the KSA-AMLL instructs the General Prosecution and Investigation Authority (GPIA) to investigate and prosecute ML/FT crimes. Article 11 of the KSA-AMLL establishes an FIU "to confront money laundering" and to serve as a clearing-house for all information relating to AML-CTF.

Although SAMA is not directly charged with criminal law enforcement, it is expected to play a role in the enforcement community. Its Charter grants it broad supervisory powers over the Saudi financial system. As the regulatory and supervisory authority over commercial banks, it is charged with preventing terrorists from exploiting the Saudi financial system and ensuring that banks follow AML-CTF regulations. The banking control department, under the direction of deputy governor of SAMA, is responsible for supervising banks' compliance with SAMA circulars and KSA laws and regulations. It is divided into sub-departments, such as the banking inspection department, the banking supervision department and the banking technology department.

We have found Saudi Arabia to be in partial compliance with this principle from a legal perspective.

The reason we consider Saudi Arabia only partially compliant with this principle is a lack of clarity regarding the role each of the designated authorities plays within the enforcement community, as well as the non-designation of authorities for a number of important functions specified in the KSA-AMLL.

a. *Interaction with Ministry of Interior.*

Although not specified in the laws to which we have had access, the police forces under the Ministry of the Interior also play a role in enforcement of the criminal sanctions provided for by the

[38] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex [X].

AML-CTF.[39] It is not clear to us how the Ministry of Interior is expected to interact with the above-mentioned enforcement authorities.

b. *Coordination.*

It is unclear whether these laws provide for an adequate level of coordination between the GPIA, the FIU, SAMA, and other enforcement agencies. It is important that coordination mechanisms be specified as part of the designation of authorities.

c. *Lack of Designations.*

In a number of instances, the KSA-AMLL establishes legal powers or obligations without designating the authority in which such power or obligation is to inhere. For example, Article 12 of the KSA-AMLL authorizes the FIU to "direct the concerned authorities to attach properties, proceeds and instrumentalities" upon "confirming" a suspicion of ML/FT conduct. Similarly, Article 15 instructs "the concerned authorities" to dispose of confiscated properties, proceeds and instrumentalities the destruction of which has not been ordered by the court.

We expect that these ambiguities will be resolved by the forthcoming Implementation Rules to the KSA-AMLL. Until such Rules are promulgated, however, the lack of designations for these ancillary powers and obligations will remain a potential impediment to the proper functioning of the law enforcement community as regards ML/FT offenses.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. Our information does indicate, however, that members of the Saudi AML-CFT criminal law enforcement community are aware, to various degrees, of the new designations of authority.[40]

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

[39] Interview, Senior U.S. Government official, 11/21/03
[40] Interview, Senior U.S. Government official, 11/21/03

Principle 28: Authority to Obtain Documents and Information

Standard:

We have used FATF Recommendation 28[41] for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information tends to indicate Saudi Arabia's substantial compliance.

From an enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information tends to indicate Saudi Arabia's full compliance in the banking sector.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information tends to indicate Saudi Arabia's full compliance in the banking sector.

Law:

Article 8 of the KSA-AMLL requires Institutions to provide judicial and other concerned authorities with records and documents subject to applicable regulations. In the banking sector, Article 18 of the Banking Control Law (the "KSA-BCL") authorizes SAMA to conduct audits of any bank; Article 17 of the same law authorizes SAMA to require any bank to submit any statement according to SAMA forms.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's substantial compliance with the principle.

We have not been able to view the Saudi laws pertaining to general search and seizure authorizations, subpoena powers and the like. Although the laws cited above provide adequate authority to obtain documents and information from Institutions in the normal course of events, we note (1) that Institutions are defined to exclude non-profit organizations, and (2) that the laws cited above do not provide for search and seizure powers.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. Our limited information tends to indicate Saudi Arabia's full compliance with the principle in the banking sector.

According to Kevin Taecker, a former SAMBA official, SAMA installed an advanced inter-clearing banking system in 1998-99 to give it real-time access to transactions, in an effective utilization of its information-gathering authority.[42] However, we have not been able to obtain

[41] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.
[42] Interview with Kevin Taecker on 11/11/03.

systematic data on the use by law enforcement agencies of their authority to require documents and information, and we have not been able to obtain even anecdotal data on such use by law enforcement agencies outside the banking sector.

We have also been unable to obtain data on instances of non-compliance with requests for information, and any sanctions applied in such instances.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. Our limited information tends to indicate Saudi Arabia's full compliance with the principle in the banking sector.

We have anecdotal evidence suggesting that SAMA's authority to obtain documents and evidence has contributed to its effectiveness as a regulator. Taecker advised us that SAMA has excellent intelligence, and is highly aware of developments at Saudi banks. According to him, moreover, bank officials comply with any demand for information because SAMA is able to apply heavy sanctions.[43]

[43] Interview with Kevin Taecker on 11/11/03.

Capacity of Authorities

Compliance with international AML/CFT standards entails ensuring the practical capacity of law enforcement agencies to carry out their functions. Most importantly, if designated authorities do not have sufficient human and material resources, their work may be seriously hampered, regardless of the legal authority afforded them. Such resources should be reflected in the form of adequate staffing levels, professional training specific to individual responsibilities, and adequate budget levels to fund requisite activities in countering money laundering and terrorist financing.

Absent adequate staffing levels, enforcement agencies may lack the manpower necessary to monitor and prosecute a significant volume of the money laundering and terrorist financing activities in the jurisdiction. Poor training of employees of the designated authorities may leave them unprepared to carry out the complex analysis necessary to unravel, understand and successfully prosecute sophisticated webs of money laundering and terrorist financing. Inadequacy in allocated budgets, meanwhile, may leave the designated authorities unable to acquire and utilize technological and other tools that can serve as "force multipliers" in both their monitoring and prosecution activities.

Another factor that could obstruct efficient and appropriate functioning of the designated authorities is a lack of coordination among themselves. A measure of the capacity of criminal law enforcement authorities, therefore, must include an assessment of the mechanisms that exists to ensure proper coordination within the enforcement community.

Finally, serious problems could also arise if the designated authorities do not have access to updated information tracking and statistics compiling systems. In light of the sophistication and creativity of prime actors in the money laundering and terrorist financing fields, law enforcement authorities without the institutional or technological ability to track information flow and analyze trends could be at a severe disadvantage in attempting to disrupt ML/FT activity.

Principle 30: Resources Available to Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 30[44] for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

We have not been able to identify any appropriations bills or similar legislative actions outlining resources allocated to various agencies. We note that such legislative actions are not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

In order to adequately assess the capacity of Saudi Arabia's criminal enforcement institutions, we attempted to gather data on the budgets of the relevant institutions and divisions, the number of personnel dedicated to AML/CTF enforcement, and the level of training received by such personnel. Such data could be compared both to analogous figures from other countries and to data from previous years in Saudi Arabia, to provide a clear and sophisticated picture of Saudi efforts to counter ML/FT offenses.

We have found no information available on budget and staffing levels of any of Saudi Arabia's criminal enforcement agencies. We have uncovered anecdotal data on training practices. This anecdotal data confirms the Saudi government claim that it initiated a program to train judges and investigators in AML-CTF issues in February 2003.[45] We have no information on the content of

[44] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.
[45] "Initiatives and Actions Taken by the Kingdom of Saudi Arabia in the Financial Area to Combat Terrorism," Kingdom of Saudi Arabia, 2003. p. 6. Interview, Senior U.S. Government Official, 11/21/03

the training program or on how many people have been trained. From Congressional testimony, we have learned that the Mabahith are engaged in a joint CTF training effort with the FBI.[46] As of September, 2003, 20 Mabahith agents were being trained.[47] We have not been able to obtain information on the content of the program.

As an alternative measure of the resources allocated to Saudi criminal law enforcement authorities, we endeavoured to acquire data on the volume and quality of law enforcement activity to date in the AML/CTF field. Such data would include statistics on criminal trials for money laundering, sentences handed down for terrorist financing, assets seized, and so forth. Absent evidence of legal action by the enforcement authorities, even a record of the number of suspicious transaction reports filed by Saudi banks with SAMA could serve as an indirect measure of the resources devoted by the Saudi government to AML/CTF measures.

Again, we have found very little data available. The Saudi government has released figures claiming to have questioned over 2,000 individuals and arrested 250.[48] These actions were taken in the course of combating terrorism generally, not terrorist financing in particular. No statistics were available on the application of legal sanction to financial institutions for non-compliance with AML/CTF regulations. Former bankers in Saudi Arabia indicated, in our interviews with them, that they were only aware of legal action being taken in cases of fraud, and even those cases were rare.[49]

An accounting of assets frozen is among the few points of solid data available. The Saudi government declared that, as of December 2002, it had investigated "many" accounts, and frozen 33 of them.[50] These accounts belonged to three different individuals and contained funds totaling $5,574,196. Figures provided to the U.S. Senate in October 2003 put the Saudi freezes at 41 bank accounts belonging to 7 individuals for a total of $5,697,400.[51] This figure represents 4% of the total terrorist funds frozen worldwide since September 11, 2001.[52] In the absence of more detailed information on the scope of law enforcement activity that led up to these asset freezes, it is difficult to base on them an estimate of the resources allocated to the enforcement agencies responsible for the freezes.

In short, outside of Saudi declarations, we do not have enough information to verify whether the Saudis have put in place adequate resources to conduct effective money laundering and terrorist financing investigations or launch prosecutions. Nor can we attempt to assess whether the resources allocated are adequate by reviewing Saudi results, as data on legal action is also lacking. Examples of unanswered questions include:

- how many people make up the FIU?
- what is the FIU's budget?
- what are the qualifications of the staff making up the FIU and GPIA?

---

[46] John Pistole, testimony, House committee on financial services testimony on Sept. 24, 2003
[47] John Pistole, testimony, House committee on financial services testimony on Sept. 24, 2003
[48] "Initiatives and Actions Taken by the Kingdom of Saudi Arabia in the Financial Area to Combat Terrorism," Kingdom of Saudi Arabia, 2003. p. 4.
[49] Interviews with a Saudi banker and a former SAMBA officer.
[50] "Initiatives and Actions Taken by the Kingdom of Saudi Arabia in the Financial Area to Combat Terrorism," Kingdom of Saudi Arabia, 2003. p. 6.
[51] Brisard, Jean-Charles. Testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs, October 22, 2003.
[52] Brisard, Jean-Charles. Testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs, October 22, 2003.

- how many people in SAMA are devoted to combating terrorist financing?
- what is the status of the relevant training programs?
- what level of training is being offered?
- how many criminal trials for money laundering or terrorist financing have taken place?
- what percentage of STRs resulted in legal action?
- how many sentences were handed down?
- how severe were these sentences?

Principle 31: Coordination Among Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 31[53] for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the KSA-AMLL establishes the FIU as a clearing-house for ML/FT information, but does not specify its role vis-à-vis other actors in the law enforcement community. Apart from the FIU, we have not found any legal basis for any coordinatory mechanism in the AML/CTF enforcement community. For instance, the KSA-AMLL designates the GPIA as the enforcement agency tasked with prosecuting money laundering and terrorist financing offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies. SAMA's guidelines, directed at banks, provide only oblique references to SAMA's cooperation with other agencies.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

Apart from the FIU, we have not found any legal basis for any coordinatory mechanism in the AML/CTF enforcement community. For instance, the KSA-AMLL designates the GPIA as the enforcement agency tasked with prosecuting money laundering and terrorist financing offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies. SAMA's guidelines, directed at banks, provide only oblique references to SAMA's cooperation with other agencies. We note that such legislative basis for coordination is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

---

[53] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

We do not have information on cooperation among and between Saudi enforcement agencies or regulatory bodies in either the enforcement sphere or in developing new rules and regulations. Examples of types of data that would be helpful include data on the number of STR's filed or other information showing cooperation between supervisors, the FIU, compliance officers in financial institutions, and SAMA.

Principle 32: Information Tracking by Criminal Law Enforcement Authorities

Standard:

We have used FATF Recommendation 32[54] for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the KSA-AMLL directs the FIU to "be responsible for receiving and analyzing reports and prepare reports on suspicious operations from all Financial and Non-Financial Institutions."

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

Apart from the oblique mention of "preparing reports" in Article 11 of the KSA-AMLL, we have not found any legal basis for any information tracking or statistic compiling mechanism in the AML/CTF enforcement community. We note that such legislative basis for information tracking is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Although the Saudis have cited the amount of terrorist assets frozen in various press releases, we have been unable to obtain any evidence that demonstrates that an orderly system for tracking this data exists. Furthermore, we are not aware of any money laundering or terrorist financing prosecutions having been made public. Thus, we are unable to evaluate if an effective record keeping system pertaining to this crime fighting data is being maintained.

---

[54] The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

We note, however, that SAMA has committed to implementing such a system: in Article 4.1 of the SAMA-AMLCTF, the agency states that it will "ensure that all banks are kept updated with the latest information on efforts to combat all economic crimes including anti-money laundering within Saudi Arabia and will distribute, on a half yearly basis, statistical information covering the total number of cases reported by region, currency, method, amount, lessons learnt, etc." Should this commitment be fulfilled by SAMA, it would constitute a significant step toward the establishment of an information tracking system compliant with this principle.

Conclusions – Criminal Law

Our review and analysis of Saudi Arabia's criminal law system as regards ML/FT offenses has highlighted a number of areas in which that system is fully or substantially compliant with relevant international standards. However, there are also several issues of concern, which will require continuing attention:

1. Saudi Arabia's compliance with international standards on the definitional scope of the criminal offense of terrorist financing is unsatisfactory. Although Saudi Arabia has expressly outlawed the financing of terrorism, we have not been able to find a Saudi legal definition of the predicate offense of terrorism itself. Moreover, Saudi Arabia is not a signatory of the UN CTB Convention, which provides an internationally accepted definition for an important type of modern terrorism. The regional anti-terrorism conventions to which Saudi Arabia is a party contain definitions of terrorism that are inadequate in terms of both geographic reach (limited to the States Parties themselves) and scope of subject matter (excluding acts of "armed struggle against occupation"). This lack of clarity in Saudi Arabia's legal definition of terrorism has the potential to undermine severely its prosecution of terrorist financing.

Another, related concern has to do with the vagueness of Saudi Arabia's definition of financing. In contrast to the detailed language in relevant international instruments and conventions – including UNSC R1373 – outlining the definition of financing, Saudi Arabia has chosen not to define the term. This contrasts with Saudi Arabia's commendable specificity in defining money laundering based on the language in relevant international instruments and conventions.

2. The lack of transparency regarding Saudi Arabia's enforcement of its criminal laws relating to ML/FT is another main source of concern. This opaqueness prevented us from examining the human and material resources of the various enforcement agencies, as well as their ability to work with each other. In addition, it prevented us from analyzing the enforcement and prosecution activity to date in the AML/CTF field. By blocking both these lines of inquiry, the lack of transparency has left us – and, by implication, other open-source analysts, as well as the general public – unable to assess or verify the extent to which Saudi Arabia's criminal law enforcement efforts are compliant with international standards, and indeed the seriousness of such efforts. Beyond the obvious nondesirability of opaqueness on these important issues, we are concerned that this lack of publicly available information may undermine the deterrent effect of the Saudi AML/CTF criminal law regime.

3. A third major source of concern is the apparent exclusion of non-profit organizations, such as charities, from criminal liability as legal persons. We appreciate the fact that a charity's officials are subject to criminal liability for ML/FT offenses as natural persons, and that such personal liability will doubtless impact the use of charities as ML/FT conduits. Nonetheless, it is important that the non-profit organizations themselves, as legal entities, be subject to criminal liability, especially in light of the important role that charities play in a devout Islamic society. Since such legal entity liability is extended to financial and commercial enterprises, we do not understand the failure to extend it equally to non-profit organizations.

Regulatory Regime

A vital component of a country's AML/CTF effort is its regulatory regime. This institutional structure creates a body of rules, regulations and requirements that delineate the responsibilities of financial, commercial, non-profit and informal entities. A regulatory regime also authorizes institutional oversight over these entities. Consistent implementation and enforcement by regulators creates a deterrent effect. In addition, the thoroughness with which a country monitors and sanctions ML/FT activity sends an important public message about its determination to eradicate such activity, while stigmatizing those who engage in it.

This chapter will examine six significant aspects of the regulatory regime component of Saudi Arabia's AML/CTF effort:

- Institutional measures to combat AML-CTF: Countries need to create an efficient institutional infrastructure in order to handle reporting, supervision, implementation and enforcement of the AML-CFT regulations by financial, commercial, non-profit and informal entities. In addition, appropriate administrative capacity and competent enforcement authorities are necessary to eliminate terrorist financing and identify, prosecute and sanction offenders.
- KYC requirements regarding customer identification and due diligence: Knowing the client is the cornerstone of an effective AML and CTF regime. Financial and non-financial institutions are vulnerable if they don't have a solid knowledge of their clients, the clients' source of funds, their business activities, and the control structure of the clients' entities. In addition, there are specific risks posed by special categories of clients, such as Politically Exposed Persons and Correspondent Banks.
- Monitoring and reporting transactions: The risk of money laundering and terrorist financing cannot be effectively reduced without ongoing monitoring of the transactions. If the institutions do not have the means to detect suspicious transactions, including systems (technology), adequate staff and knowledge, they could fail in their duty to report suspicious activity. The monitoring and reporting of transactions should be tailored for the level of risk of the account, implying a higher level of monitoring for high-risk accounts.
- Retention of Records: Records of transactions and identification data are necessary documents in order to reconstruct transactions and follow the money trail in an investigation. If such documents are destroyed, not maintained long enough, or are not made available to competent authorities, then the reconstruction of evidence is seriously impaired.
- Non-financial sector: Non financial institutions such as real estate businesses, law practices, precious metals and precious stone dealers are often used by criminals as conduits for laundering money or financing terrorism. Therefore, the same standards of regulation, supervision and due diligence must be applied to non financial institutions as they are applied to financial institutions.
- Non-profit sector (Charities): Non profit institutions play an important role in Saudi society. A variety of ministries and agencies have authority over the regulation of this sector. Delineations of authority are unclear. Given the recent history of abuse of charitable funds this sector requires analysis. Supervision and due diligence must be applied to non profit institutions as they are applied to financial institutions.

Institutional Measures to Combat AML-CTF

Financial and non-financial entities are subject to money laundering and terrorist financing risks resulting from inadequate controls and procedures. The country's secrecy laws as applied to financial institutions could interfere with the implementation of Anti-Money Laundering policies. This problem is especially relevant in cooperation with authorities and sharing information between institutions.

In addition to having the legal structure in place, a country needs to create an efficient institutional infrastructure in order to handle reporting, supervision, implementation and enforcement of the AML-CFT regulations by the financial institutions.

Without the appropriate administrative capacity, the competent enforcement authorities will lack the resources necessary to eliminate terrorist financing and identify, prosecute and sanction offenders.

Principle 33: Preemption of Financial Institution Secrecy Laws

Standard:

A country's secrecy law should not inhibit the implementation of the FATF Recommendations.[55]

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an implementation and enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The Regulations on Anti Money Laundering in KSA – Anti Money Laundering Law ("KSA-AMLL") mentions confidentiality provisions in Articles 8, 13, 22 and 25. Article 25 is a safe harbor for persons who violate confidentiality provisions by performing their reporting duties. SAMA's Rules Governing Anti Money Laundering and Combating Terrorist Financing ("SAMA-AMLCTF") mention the importance of confidentiality provisions throughout the document, but also include a safe harbor (Article 12.4.D and Article 13.2) for banks and bank employees that notify SAMA or the FIU (see also Standard 34).

The provisions in the KSA-AMLL are unsatisfactorily vague regarding the interplay between secrecy laws and reporting requirements. Article 8 of the KSA-AMLL instructs Institutions to provide information to judicial or other concerned authorities "as an exception to the confidentiality provisions,"[56] but subject to unspecified "applicable regulations." Article 13, expanding on the Article 8 language, specifies that information "discovered"[57] by Institutions and relating to a violation of the KSA-AMLL "may be shared with the concerned authorities" to the extent necessary for investigation or judicial action. Article 25, as a safe harbor, exempts directors, manager, employees, owners and agents of Institutions from liability for violating confidentiality provisions in the course of performing their KSA-AMLL obligations, unless they are proven to have "acted in bad faith to hurt the involved person."

The safe harbor in Article 25 is limited to carrying out the duties set forth in the KSA-AMLL. These duties include notifying the FIU of suspicious transactions (Article 7); consequently, the safe harbor appears to prevent bank secrecy laws from interfering with the initial notification of the FIU regarding suspicious transactions. The duties also include cooperating with other "concerned authorities" (Article 8, and Article 13 which appears to draw its authority from Article 8). However, since the duty of cooperation with other authorities is made contingent on following the vaguely specified "applicable regulations," we cannot assess the degree to which the safe harbor provides meaningful protection, absent an analysis of these regulations.

As regards regulations applying to the financial sector, we analyzed SAMA-AMLCTF to determine the degree to which it limits the cooperation detailed in Article 8 of the KSA-AMLL. Our analysis suggests that any cooperation other than through SAMA is forbidden by SAMA-AMLCTF.

---

[55] FATF Recommendation 4. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[56] [Translation by Prof. Hassan]

[57] [Translation by Prof. Hassan]

Article 3.11 of SAMA-AMLCTF states that "[b]anks, as directed by SAMA, should provide all relevant details and documents, as and when required. Under any circumstances, customer information should not be released to any party without SAMA's approval." This language clearly prohibits banks from sending customer information to other parties, such as law enforcement agencies, except through SAMA or with SAMA's permission.

Based on our analysis of the KSA-AMLL and SAMA-AMLCTF, we are concerned that the Saudi regulatory framework appears to exempt only interactions with SAMA and the FIU from the strictures of the financial confidentiality provisions. Although we acknowledge the efficiency and professionalism of SAMA, the inhibition of communications between banks and other enforcement agencies places unnecessary strain on SAMA as a conduit of information.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

The "safe harbor" provision as described above has been recently enacted and its implementation could not be assessed. With regards to conflicts between the country's financial institutions secrecy laws and the need to share information between institutions, Saudi Arabia's strict secrecy laws are not an exception. Switzerland, for example, has very stringent secrecy laws as well, going as far as prohibiting the sharing of information between the local branch and the overseas headquarter. However, western financial institutions operating in Switzerland often require their clients to sign a waiver in which they give the institution holding their accounts permission to share information with the parent company abroad as needed[58]. As far as we could determine, Saudi Arabia does not follow this practice.

[58] Interview with compliance officer at large international bank November 5, 2003.

Principle 34: Protection from Liability for Disclosure

Standard:

There must be legal provisions protecting financial institutions' officers from criminal and civil liability in order to ensure that suspicious activities are properly reported without the fear of personal liability for breaching client confidentiality. These provisions should cover financial institutions, their directors, officers and employees in terms of protection from criminal and civil liability for breach of any restriction on disclosure to the FIU, if the information was reported in good faith. This provision should apply even when the underlying criminal activity is not known, or whether an illegal activity actually occurred.[59]

Assessment:

From a legal perspective, the Saudi law is fully compliant.

From an implementation and enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Protection of persons from liability for reporting suspicions to the authorities is covered in Article 25 of the KSA-AMLL, and in Articles 12.4.D and 13.2 of SAMA-AMLCTF.

The KSA-AMLL provides that owners, managers, employees and agents of Institutions "shall be relieved from criminal, civil or administrative liability that may be caused by performing the duties provided for herein or by violating the provisions of confidentiality, unless it is established that they acted in bad faith to hurt the involved person" (Article 25). Meanwhile, SAMA-AMLCTF, in the context of suspicious transaction reporting, states that "[t]he notifying bank and its employees are free of any blame or charge in respect of any notification made, whether the suspicion is proved to be correct or not, as long as their notification was made in good faith" (Article 12.4.D). SAMA-AMLCTF further states, in the context of its tipping prohibition, that "[n]otification of suspected money laundering and terrorist financing cases to the authorities does not conflict with the provision of banking secrecy or customer confidentiality under the Saudi Arabian Banking Laws and Regulations" (Article 13.2).

Implementation/Enforcement:

The implementation and enforcement of the safe harbor provision is discussed under Principle 1. However, according to FATF 14a, the safe harbor provision should apply to disclosure to the FIU. In Saudi Arabia the FIU is not fully operational yet. Financial Institutions are instructed to make all the disclosures to SAMA directly, or not make any disclosures at all to any other government institution without consulting SAMA and obtaining permission from SAMA to do so.[60]

---

[59] FATF Recommendation 14a. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[60] Interview with former senior SAMBA employee, November 12 2003

Principle 35: Prohibition on Tipping Off

Standard:

Financial Institutions should not disclose the fact that information about a client is reported to the FIU.[61]

Assessment:

From a legal perspective, the Saudi law is fully compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Prohibition on disclosing the fact that a suspicious transaction has been reported to the authorities is covered in Article 9 of the KSA-AMLL, and in Article 13.1 of SAMA-AMLCTF.

The KSA-AMLL requires that Institutions and their employees "shall not alert or permit to alert clients or other related parties about suspicions regarding their activities" (Article 9). SAMA-AMLCTF provides that "[b]anks shall not under any circumstances inform customers of their suspicion or of their notification to the authorities. Extreme caution must be exercised when dealing with these customers" (Article 13.1).

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

[61] FATF Recommendation 14b. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

Principle 36: Development of Internal AML and CFT programs

Standard:

Financial Institutions should be mandated to develop internal AML and CTF programs that should include: internal policies, procedures and controls, employee screening procedures, ongoing training program, and an audit function to test the system.[62]

Assessment:

From a legal perspective, the Saudi law is largely compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Both KSA-AMLL and SAMA-AMLCTF cover this principle. Article 10 of the KSA-AMLL applies both to financial and non-financial institutions.

Saudi programs against ML and TF include:

i) Development of internal policies – This is covered by KSA AMLL, Article 10, a) and SAMA-AMLCTF 6.7. However, there is no provision for screening of employees. In Guidelines for Prevention of Money Laundering issued by SAMA in 1995 we found a provision regarding promoting Saudi nationals in positions sensitive to money laundering such as cashiers, tellers, etc, but no specific requirements with respect to screening of employees prior to hiring or on an ongoing basis.

ii) Ongoing employee training program – This is covered by KSA-AMLL, Article 10, c) and SAMA-AMLCTF 5.2. Article 10 specifies that ongoing training programs should be developed for "specialized" employees, such that they would be able to identify and combat money laundering. This article does not cover all employees working for a financial or non-financial institution. Industry best practices recommend all employees should have ongoing training so that each employee is aware of and able to recognize and report suspicious activity. SAMA-AMLCTF 5.2 recommends training for all employees, but only front line and account opening personnel are subject to full training to be planned through the bank's annual compliance plan.

iii) Audit function to test the system – This is covered by KSA-AMLL, Article 10, b) which only requires that the auditing function supervise the "availability of basic requirements to combat ML". Compliant as per SAMA-AMLCTF 6.8.

iv) External auditors as per Basel 59 – No provision was found in the KSA- AMLL or SAMA-AMLCTF, however this principle is covered in the SAMA Guidelines for Prevention of Money Laundering dated 1995.

Enforcement:

[62] FATF Recommendation 15, Basel 18,19, 55-59. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1and 3.

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

In interviews with former bank officers from KSA, we learned that the banks set up as joint ventures with a western bank are required to follow the internal policies of the western counterpart. According to these bank officers, these internal policies are very strict, in most cases exceeding the requirements of the national laws. We have not received the same degree of assurance regarding the purely Saudi banks.[63] We have not been able to assess compliance with this principle from an implementation and enforcement perspective by financial institutions other than banks or by the non-financial institutions.

[63]Interview with former senior SAMBA employee, November 12 2003, and Interview with compliance officer at large international bank October 7, 2003.

Principle 37: Foreign Branches and Subsidiaries

Standard:

The standards employed by financial institutions in combating money laundering and terrorist financing should apply to branches and subsidiaries located abroad.[64]

Assessment:

From a legal perspective the Saudi law is partially compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

There is no provision in the KSA-AMLL for foreign branches and subsidiaries.

SAMA-AMLCTF 5.4 recommends that standards followed by local financial institutions are also applied to branches and majority owned subsidiaries located abroad. From a legal perspective, SAMA is in compliance with the FATF requirements.

FATF further recommends that in cases in which local laws and regulations prohibit this implementation, the parent company should be notified. SAMA does not have a provision for this recommendation.

Furthermore, in 5.4 SAMA-AMLCTF specifies that "where local ML and TF legislation is in effect, this must be adhered to". The implication is that foreign branches and subsidiaries could have lower AML standards than the Saudi parent company, for as long as local legislation is adhered to. This implication could be also inferred from section 6.17.7 of SAMA-AMLCTF: "where a foreign branch, subsidiary or associate refers business to a bank in Saudi Arabia [...] the bank should [...] determine whether it complies with Saudi Arabian laws and regulations".

This contradicts Basel 66, which require that the higher standard of the two be applied in cases in which the standards of the two countries differ. In this respect, provision 5.4 of SAMA-AMLCTF is non-compliant.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

[64] FATF Recommendation 22, Basel 63-69. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Principle 38: Effective Regulatory Sanctions

Standard:

Sanctions must be in place in order to strengthen the enforcement of the regulations, including criminal, civil and administrative, to be applied to legal and natural persons The punishment for non-compliance with anti-money laundering or terrorist financing requirements must be clearly stated in order to achieve their purpose of deterrence and dissuasion.[65]

Assessment:

From a legal perspective the Saudi law is fully compliant.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Sanctions relevant to the AML/CFT regulatory regime in Saudi Arabia are provided in Articles 16-20 of the KSA-AMLL, and Articles 22 and 23 of the Banks Control Law (the "KSA-BCL").

Under the KSA-BCL, SAMA is authorized to sanction violations of its regulation by suspending or discharging any bank director or employee, suspending a bank's loan-granting and deposit-accepting authority, and revoking a bank's license (Article 22). In addition, individuals responsible for a violation may be sanctioned with a fine of up to S.R. 5,000 (US $1,333) (Article 23(5)).

Under the KSA-AMLL, the penalty imposed on Institutions that commit ML/FT offenses – which occurs when "such offenses [are] committed in their name or to their account" (Article 3) – is "a fine ranging from SR 100,000 [US $26,667] up to the value of the property involved in the offence" (Article 19). The administrative obligations in Articles 4-10 are backed by a sanction of "a jail penalty up to 2 years or a fine up to SR 500,000 [US $133,333]" (Article 18). Finally, Article 20, a type of basket provision, states that "[a]nyone violating a provision not stated hereof shall be subject to a jail penalty up to six months and a fine up to SR 100,000 [US $26,667] or to either punishment." See also analysis of criminal sanctions on natural persons, under Principle 17a.

It is also noteworthy that, under Saudi *shari'a*, the concept of *ta'azir* ("discretionary penalty" offenses) permits a court to extend the reach of the sanctioning power beyond that set forth in the enacted law. With regard to *ta'azir* offenses that violate the public interest (*al-maslaha al-'amma*), *shari'a* principles allow an act that is otherwise permissible to be deemed an offense if the context renders such conduct harmful to public interest. This is an exception to the general rule that only conduct forbidden by textual authority can be sanctioned.[66]

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have been unable to determine whether law enforcement and prosecutorial agencies

[65] FATF Recommendation 17. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[66] Criminal Justice in Islam: Judicial Procedure in the Shari'a 71-72 (2003, Muhammad Abdel Haleem et al. ed.); Mohamed S. El-Awa, Punishment in Islamic Law: A Comparative Study 114-16 (1981).

are seeking to take full advantage of the punitive range
provided by the KSA-AMLL's sanctions provisions for the administrative offenses specified in that law. Additionally, we have not been able to obtain any systematic data on SAMA's use of its sanctioning power under the KSA-BCL.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. We have been unable to assess the range of penalties meted out by the Shari'a courts for regulatory offenses under the KSA-AMLL, and the extent
of any deterrence engendered by such penalties. However, anecdotal evidence does suggest that, within the financial sector, banking officials are highly aware of, and deterred by, SAMA's sanctioning power.

We have had inconsistent reports on whether the sanctioning power inducing such deterrent effect is indeed the sanctioning power granted to SAMA by law, or whether it derives from SAMA's [political] influence on other law enforcement agencies with different sanctioning powers.

Principle 39: Establishment of Guidelines for Creation of an AML Regime

Standard:

The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.[67]

Assessment:

From a legal perspective the Saudi law is fully compliant.

From an implementation perspective the Saudi law is fully compliant with respect to financial institutions. We have not been able to verify Saudi Arabia's compliance with this principle with respect to non-financial institutions.

Law:

The Saudi Government has established guidelines for financial institutions and designated non-financial institutions to follow to create an effective AML-CTF regime. The KSA-AMLL, the SAMA-AMLCTF, and the Banking Control Law all set forth requirements for institutions to follow. The SAMA-AMLCTF regulations are especially relevant in this regard. In addition to mandating specific actions that institutions must take and establish parameters for such things suspicious transactions and know-your-customer policies, they provide recommended preventive procedures and offer an appendix on indicators of ML or TF activity.[68]

Enforcement:

Enforcement issues are not applicable to this standard.

Implementation:

The guidelines have been established.

We were unable to assess compliance from an implementation perspective with respect to assistance and feedback to financial and non-financial institutions by the competent authorities.

[67] FATF Recommendation 25. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[68] Kingdom of Saudi Arabia, SAMA Banking Inspection Department, Rules Governing Anti-Money Laundering and Counter-Terrorist Financing, May 2003, 27-28 and 30-35.

Principle 40: Establishment of an FIU

Standard:

Countries should establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of Suspicious Transaction Reports (STRs) and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR[69].

The Egmont Group of Financial Intelligence Units also provides standards and statements of purpose for FIU's.

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the KSA-AMLL establishes the Saudi FIU. However, the law states that "The Location of its [the FIU's] head office, its structure, its power and method of exercising its duties and connections" will be outlined in the implementation rules related to the AML laws. These rules were expected to be released by the end of November 2003, but to date, are still not available to us. The KSA-AMLL also designates the General Prosecution and Investigation Authority ("GPIA") as the enforcement agency tasked with prosecuting ML/FT offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies.

Article 4.1 of the SAMA-AMLCTF requires all local banks to report suspicious transactions to both the Saudi FIU and to SAMA.

We do not have enough data to assess Saudi Arabia's progress in this area. Most importantly, we do not have the implementation laws mentioned in Article 11.

In lieu of an evaluation, it is useful to briefly outline the major elements that we would expect to see in the new implementation rules as defined by the FATF methodology. Specifically, the new central body should meet the Egmont Group definition of an FIU as well as perform the mission outlined in the Statement of Purpose of the Egmont Group of FIU's.[70] Furthermore, the FIU should have the authority to request additional information from reporting parties, have access to financial, administrative and law enforcement information on a timely basis, be authorized to order sanctions against reporting institutions that fail to comply with their obligations, and be authorized to share information with both local and international law enforcement agencies.

---

[69] FATF Recommendation 26. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[70] Statement of Purpose of the Egmont Group of Financial Intelligence Units, The Hague, June 13, 2001, http://www1.oecd.org/fatf/pdf/EGstat-200106_en.pdf (last visited on December 5, 2003)

It is important to note that some of the basic steps towards developing an FIU are already in the current laws. Specifically, the FATF methodology states that all financial institutions should be required to send any Suspicious Transaction Report (STR) to the FIU. Saudi institutions are already obligated to do this under Article 7 of the new Anti Money Laundering Laws. Furthermore, the FIU should issue guidelines for identifying complex transactions. Currently SAMA, the Saudi central bank, seems to be effectively fulfilling that role by issuing documents such as The Rules Governing Anti Money Laundering and Combating Terrorist Financing, which it released in May 2003.

Implementation/Enforcement:

The Saudi Government has recently created an FIU within the Ministry of Interior.[71] We understand that this FIU is not yet fully functional, and that SAMA is currently fulfilling this role as a central clearinghouse for information on money laundering and terrorist financing.[72] We have no data on resource allocations or implementation of the new AML laws and thus cannot assess Saudi compliance with this standard. Key missing pieces of information include: the power of the FIU to collect information from financial and non-financial institutions, the budget of the FIU, the number of staff allocated to the FIU as well as the level of staff training and the degree of coordination between other government authorities and the FIU.

[71] Interview, Senior U.S. Government Official.
[72] Interview, Senior U.S. Government Official.

Principle 41: Supervisory Authority

Standard:

Supervisors of the financial sector should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.[73]

Assessment:

From a legal perspective, we have found Saudi Arabia to be substantially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 18 of the Banking Control Law (the "KSA-BCL") authorizes SAMA to conduct audits of any bank. Article 17 of the same law authorizes SAMA to require any bank to submit any statement according to SAMA forms.

Article 25 of the KSA-AMLL relieves owners, managers, representatives and employees of Financial and Non-Financial Institutions from liability for violating confidentiality provisions in the course of obeying the KSA-AMLL, unless they were acting in bad faith to hurt the involved person.

Sanctions:

Under the KSA-BCL, SAMA is authorized to sanction violations of its regulations by suspending or discharging any bank director or employee, suspending a bank's loan-granting and deposit-accepting authority, and revoking a bank's license (Article 22). In addition, individuals responsible for a violation may be sanctioned with a fine of up to S.R. 5,000 (~ US $1,333) (Article 23(5)).

Under the KSA-AMLL, the administrative obligations in Articles 4-10 – which include reporting requirements and a duty to make certain documents available to supervisory authorities – are backed by a sanction of "a jail penalty up to 2 years or a fine up to SR 500,000 [US $133,333]" (Article 18).

Thus, SAMA appears to have the authority to compel banks to provide it with information as well as the power to sanction non-cooperation directly through the KSA-BCL, or indirectly by subjecting the non-cooperating entity to sanction under the KSA-AMLL.

Implementation/Enforcement:

Saudi law may vest the supervisory authorities with the necessary powers, but there is little indication that those authorities are exercising this power. We have yet to see, outside of occasional Saudi announcements about single incidents, concrete evidence of fund seizures, terrorist financing prosecutions, or sanctions placed on any Saudi banks for violating the new AML laws. Nor do we

[73] FATF Recommendation 29. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

have information on how often the Saudi government requests assistance from financial institutions for AML-CTF, and how often those requests are satisfied. Accordingly, we are unable to verify Saudi Arabia's compliance with this principle from the enforcement and implementation perspectives.

Principle 42: Resources Available to Regulatory Supervisors

Standard:

Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.[74]

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective.

Saudi Laws and Regulations do not set standards for financial, human or technical resources for government authorities. Article 10 of the KSA-AMLL instructs the relevant financial and non-financial institutions to employ qualified personnel to implement programs to combat money laundering and to provide specialized employees with continuing training about new ways and new technologies to fight money laundering and terrorist financing; however, no mention is made of the human resources available to the supervisory authorities. We note that such legislative specifications are not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

The financial and human resources discussed in this principle are key measures of Saudi Arabia's progress in combating terrorist financing. In order to adequately assess the capacity of Saudi Arabia's regulatory institutions, it is vital to know what the budgets of the relevant institutions and divisions are, how many personnel are working on AML/CTF issues, and what level of training they have received. Such information could then be compared to data from past years, to measure changes that might reflect a new awareness of the problem of terrorist financing; it could also be compared against benchmarks established by other countries.

Unfortunately, no information is available on budget and staffing levels of any of Saudi Arabia's regulatory authorities. A small bit of information is available on training practices. SAMA runs the Institute for Banking, which is the recognized qualifications and accreditation body for

[74] FATF Recommendation 30. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

professional practitioners in the banking and financial services sector in the Kingdom of Saudi Arabia.[75] It offers at least one course on Money Laundering issues to banking professionals. Further information on the activities of the institute in regard to AML-CTF is unavailable, as is any information on the training that SAMA employees themselves receive.

Though information on the capabilities of Saudi Arabia's regulatory authorities is lacking, some evidence of enforcement results would indicate that the institutions in question have the resources to fulfill their mandates. Unfortunately, hard data is unavailable in this area. Among the pieces of information that would be useful:

- Data on the number of audits that SAMA conducts and on the number of requests for information that it submits to banks.
- Data on sanctions that SAMA has leveled against banks and other institutions under its authority for failing to comply with the requirements placed upon them by AML/CTF laws and regulations. Sanctions could include fines, the dismissal of bank officials, or limits placed on a bank's future operations, up to and including the suspension of its license.
- Evidence, independent of SAMA, that the banks and other institutions are implementing the new requirements. Such compliance could be used to infer SAMA effectiveness. Such requirements include: filing suspicious transaction reports; establishing a Money Laundering Compliance Unit; retaining records for the appropriate period; establishing sound 'know-your-customer' practices. It must be noted, however, that number of STRs is not a good measure of progress on AML/CTF. It is impossible to say if a decrease in STRs over time means that there is less suspicious activity or that more of it is going undetected.

Though solid information is lacking, some anecdotal evidence casts a positive light on SAMA's general level of regulatory capability. Interviews with former employees at the Saudi-American Bank (SAMBA) and with Americans with significant experience in Gulf banking indicate that SAMA is held in high regard in the Saudi financial services community. Its personnel are thought to be professional, competent, and dedicated. Such evidence, however, lacks the comfort that would be provided by more substantial measures of capability.

[75] The Institute of Banking Website <http://www.iob.com.sa/index.php?id=10&on=10>

Principle 43: Cooperation Among Regulatory Bodies

Standard:

Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place to enable them to co-operate, and where appropriate, co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.[76]

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The KSA-AMLL establishes the Saudi FIU, but defers definition of its powers and functions to the Implementation Rules, which we have not been able to obtain. Article 28 of the KSA-AMLL states that the Minister of Interior should cooperate with the Minister of the Economy and the Minister of Finance in creating the Implementation Rules for the KSA-AMLL. The KSA-AMLL also designates the General Prosecution and Investigation Authority ("GPIA") as the enforcement agency tasked with prosecuting money laundering, terrorist financing offenses, but does not describe any mechanisms for coordination between the GPIA and other agencies. SAMA's guidelines are directed at banks, and provide only oblique references to SAMA's cooperation with other agencies. We note that such legislative basis for coordination is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

According to an interview with a senior compliance officer, SAMA does take international best standards into account when developing its rules and regulations.[77] However, we do not have information on cooperation among and between Saudi enforcement agencies or regulatory bodies in either the enforcement sphere or in developing new rules and regulations. For example, we have not

[76] FATF Recommendation 31. [The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[77] Interview with a former bank officer from KSA, November 2003

been able to obtain data on the number of STR's filed or other data showing cooperation between supervisors, the FIU, compliance officers in financial institutions, and SAMA – data that would have been helpful in assessing compliance.

Finally, it is unclear to us how SAMA coordinates with the FIU regarding Suspicious Transaction Reports, which both agencies may receive.

Principle 44: Collecting and Maintaining Statistics

Standard:

Countries should ensure that their competent authorities could review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated and on money laundering and terrorist financing investigations.[78]

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

The enforcement perspective is not relevant to this principle.

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

An effective information tracking system is an important part of the FIU. Tracking the number of STRs by specific banks allows an FIU to examine if there are any banks under its jurisdiction that are underreporting suspicious transactions. Furthermore, authorities can also compare the number of AML/CFT investigations launched as well as the number of STRs filed to similar statistics in other countries. By doing so they can measure the effectiveness of the system that is in place and see if their results demonstrate an appropriate level of reporting and investigation, vis-à-vis the requirements of international standards.

Article 11 of the new AML laws stipulates the creation of an FIU[79]. The specification of the exact nature, powers, and obligations of the FIU is deferred to the Implementation Rules, which we have not been able to obtain. Per Article 11, the FIU will be in charge of receiving and analyzing suspicious transaction reports[80]. Article 4.1 of the SAMA Rules Governing AML-CTF states that a copy of these reports will be forwarded to SAMA.[81] SAMA will keep statistical information on the total number of cases by region, currency, method, amount, and lessons learned. It will distribute this information to banks on a semi-annual basis[82].

Although the lack of rules regarding the FIU's operation is a concern, it is likely that the FIU's information tracking requirements will be fully outlined in the implementation rules document, associated with the new AML laws. Once the rules are published it will be important to evaluate the record keeping requirements of the FIU.

Also, we note that legislative basis for information tracking is not necessary to compliance with this principle, but would merely serve as evidence attesting to compliance.

---

[78] FATF Recommendation 32. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[79] Kingdom of Saudi Arabia, Regulations on Anti Money Laundering in KSA, Anti Money Laundering Law, August 2003, 4.

[80] Ibid 4

[81] Kingdom of Saudi Arabia, SAMA Banking Inspection Department, Rules Governing Anti-Money Laundering and Counter-Terrorist Financing, May 2003, 11.

[82] Ibid 11.

Enforcement:

The enforcement perspective is not relevant to this principle.

Implementation:

From an implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle. Our limited information indicates that Saudi Arabia is partially compliant with this principle, due to the role played by SAMA.

In the absence of an operational FIU, SAMA has taken on many of the roles that will eventually be transferred to the FIU. However, we have not been able to obtain any documents that demonstrate that SAMA or any other organization has been keeping track of these types of statistics.

KYC Requirements Regarding Customer Identification and Due Diligence

Knowing the client is the cornerstone of an effective AML and CTF regime. Financial and non-financial institutions could be exposed to abuses by money launderers if they don't have a solid knowledge of their clients, the clients' source of wealth and source of funds, their business activities to determine what are the normal patterns of transaction, and the control structure of the clients' entities. In addition, there are specific risks posed by special categories of clients, such as Politically Exposed Persons and Correspondent Banks.

The status of political persons allows them to take advantage of their power in either obtaining proceeds of corrupt activities or circumvent the regulatory system. Such persons are individuals who either hold or held prominent public functions, including heads of state and government, politicians and political party officials, senior government, judicial or military officials, senior executives of public corporations.
To prevent the misuse of financial and non-financial institutions by Politically Exposed Persons ("PEP"), countries should require these institutions to perform enhanced due diligence on their PEP clients.

Correspondent Banking is a relationship that enables banks to conduct business in jurisdictions in which they have no presence by using local banks in order to offer their clients products and services otherwise not offered directly. This arrangement opens the corresponding bank to money laundering risks resulting from insufficient knowledge about the clients of the respondent bank. Correspondent Banking has been identified by FATF as being one of the areas of concern with respect to money laundering.

Principle 45: Customer Due Diligence

Standard:

Financial and non financial institutions should undertake customer due diligence measures including identifying and verifying the identity of the customers, obtaining information about the intended nature of the business relationship, and creating a transaction profile for the customer. When identity could not be verified, the accounts should not be opened or the relationship should be closed[83].

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

KSA-AMLL covers the Identification requirements in Article 4, applying to both financial and non financial institutions. The law prohibits carrying out transactions under anonymous or fictitious names. The identity of the client must be verified, however the law permits the verification of the ID upon concluding the commercial transaction, contrary to the FATF Recommendation #5, which allows the timing of verification at the end of the transaction only in limited number of circumstances, such as non face-to-face business, securities transactions and life insurance business.

SAMA- AMLCTF Article 5.1 covers mandatory policies regarding customer ID, customer due diligence, and closing of the accounts in cases in which identity could not be verified. Articles 6.1 and 6.3 deal in detail with the requirement for creating a customer profile in order to determine unusual patterns of transactions for reporting purposes. These articles cover both individuals and commercial relationships.

We were unable to obtain additional ID verification rules, which are stipulated in the Implementation Rules.

Additionally, we are missing important guides for ID verification issued by SAMA to financial institutions, which are referred to in the SAMA-AMLCTF.

[83] FATF 5 and Basel 22, 23. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Articles 6.10 and 6.11 mandate Know Your Customer Standards and policy implementations. Article 6.11 makes reference to "Rules Governing the Opening of Bank Accounts in Saudi Arabia and General Operational Guidelines" issued by SAMA in 2002. **We** were unable to obtain this document in order to assess the details of compliance of this principle with the International Standards.

Article 6.13 covers due diligence for Private Banking Customers and Article 6.14 covers minimum standards for personal accounts. Both articles make reference to SAMA circulars that were not available to us, therefore a complete assessment of compliance could not be performed.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective. "However, we do have concerns that Saudi culture, which emphasizes privacy, may be a hindrance to the effective implementation of KYC standards, which require institutional intrusion into the private finances. For example, ascertaining the source of an individual's wealth is contrary to cultural norms under which people generally do not speak about a person's wealth or property. Such determinations are further complicated by the fact that Saudi Arabia has no income tax system and little to no central accounting for the wealth and property in the Kingdom."

Principle 46: Politically Exposed Persons

Standard:

Financial institutions should perform extra steps in addition to the normal due diligence measures with respect to Politically Exposed Persons:

a) have appropriate risk management system to determine whether the client is a PEP
b) obtain senior management approval for establishing a business relationship with such clients
c) asses the client's source of wealth and the source of funds
d) conduct enhanced monitoring of the business relationship.[84]

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

There is no provision in the KSA-AMLL, governing all financial and non-financial institutions, that addresses PEPs. The SAMA-AMLCTF, which governs the conducts of banks and related financial institutions, addresses PEPs in 5.1.6, 6.12.

We have found Saudi Arabia to be only partially compliant with this principle for the following reasons:

a. *Lack of coverage of the House of Saud.*

Our analysis indicates a serious deficiency in the definition of a PEP in the SAMA rules. According to SAMA, a PEP is "any individual who occupies, recently occupied, is actively seeking, or is being considered of a *senior civil position* in a government of a country, state, or municipality or any department including the military, agency, (government owned corporations, etc)".[85] [emphasis added]

By contrast, Principle 41 of the Basel CP, which we used as an international standard in assessing Saudi compliance, defines PEPs as "individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials".

The SAMA definition, by limiting its scope to "senior civil positions," does not expressly cover the House of Saud as PEPs; under the Basel CP, members of the House of Saud would be covered as either having "prominent public functions" or having the equivalent, in an absolutist monarchy, of "political" (as contrasted with "civil") positions.

---

[84] FATF Recommendation 6 and Basel 41-44. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1and 3.
[85] SAMA Rules Governing Anti Money Laundering and Combating Terrorist Financing, May 2003, 6.12.

b. *Lack of point-by-point compliance with applicable standards.*

In addition to the measures recommended by FATF, Principle 44 of the Basel CP recommends checking publicly available information to establish a client's PEP status. Principles 41-43 discuss the risk associated with PEP and suggest criminalization of corruption of civil servant and public officers in accordance with OECD Convention on *Combating Bribery on Foreign Public Officials in International Business Transactions,* adopted by the Negotiating Conference on 21 November 1997. In certain jurisdictions foreign corruption becomes a predicate offence for money laundering, therefore all AML laws and regulations apply (reporting suspicious transactions, internal freeze of funds, etc.).

A point-by-point comparison of SAMA's rules with these standards resulted in the following assessment:

- Identification of the PEP – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.12.1.
- Obtaining senior management approval for establishing a banking relationship with a PEP – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.12.1.
- Establishing the source of wealth and source of funds for a PEP – Saudi Arabia is non-compliant; we have not found a provision addressing this issue.
- Enhanced ongoing monitoring – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.12.2.
- Refusal to maintain a business relationship when there is reason to suspect corruption or misuse of public assets – Saudi Arabia is partially compliant; SAMA-AMLCTF 5.1.6 only requires the reviewing and reporting of suspicious transactions arising from known public corruption, not suspected public corruption.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Although the international standards and the industry best practices require enhanced due diligence for PEPs, we did not find evidence sufficient to confirm that the financial sector in Saudi

Arabia is adhering to these practices, in particular with respect to the royal family. When asked about the due diligence performed on PEPs, one bank officer responded that it is a known fact that their wealth was derived from oil, therefore no additional investigation of the source of wealth or the source of funds is performed.[86] A Saudi attorney suggested that a bank might find it difficult to refuse illicit requests from a PEP if that PEP is a director of the bank.[87]

[86] Interview with a bank official, November 2003
[87] Interview with a Saudi attorney, 11/11/03.

Principle 47: Correspondent Banking

Standard:

Financial institutions should implement enhanced due diligence measures when conducting business with correspondent banks.

In addition, banks should refuse to enter into a relationship or stop dealing with banks from jurisdictions with poor KYC standards, inadequate supervision, or inadequate regulations for the financial institutions. This provision includes shell banks.

In accordance with FATF Recommendations 7 and 18[88], we have used Principles 49-52 of the Basel CP for guidance in assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective, we have found Saudi Arabia to be in partial compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 6.19 of SAMA-AMLCTF covers provisions dealing with correspondent banking and prohibiting dealing with shell banks.

We do not consider the SAMA-AMLCTF's language to be fully compliant with this principle, based on the following analysis:

- Gathering information about the correspondent bank – Saudi Arabia is partially compliant, based on SAMA-AMLCTF 6.19. The language in 6.19 requires that financial institutions fully understand and document the respondent bank's management and nature of business. 6.19.5 specifies information required: location and nature of business. However, both the FATF and Basel documents suggest that additional due diligence is needed, including obtaining information about the correspondent bank's reputation, quality of supervision, whether the bank has been subject to a ML/FT investigation, its major business activities, and the purpose of the account.

- Assessing the correspondent bank's ML/FT controls – Saudi Arabia is compliant, based on SAMA-AMLCTF 6.19.4 and 6.19.5 B, C, D, E.
- Obtaining senior management approval before establishing relationship – Saudi Arabia is not compliant; we did not find a provision addressing this point.

- Documenting the responsibilities of each institution in a corresponding banking relationship – Saudi Arabia is not compliant; we did not find a provision addressing this point.

[88] FATF Recommendations 7 and 18, Basel 49-52. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1and 3.

- Verifying the identity and ongoing due diligence on third parties using the correspondent bank – Saudi Arabia is not compliant; we did not find a provision addressing this point.

- Refusal to enter into or continue a corresponding banking relationship with shell banks – Saudi Arabia is not compliant; we did not find a provision addressing this point.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 48: Non-Face-to-Face Customers

Standard:

Financial institutions should have policies in place to deal with non-face-to-face customers. The same standard of customer identification should apply to these customers as it applies to those met in person. Measures should be taken to mitigate the higher risk resulting from accepting non-face-to-face customers[89].

Assessment:

From a legal perspective, we have found Saudi Arabia to be fully compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 5.1.7 of the SAMA-AMLCTF mandates that no accounts should be opened for non-face-to-face customers. Regarding this principle SAMA goes above and beyond the FATF Recommendations and the industry practice. Accordingly, we have found Saudi Arabia to be fully compliant with this principle from a legal perspective.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

[89] FATF Recommendation 8 and Basel 45-48. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Principle 49: Introduced Business

Standard:

Financial institutions accepting introduced business may rely on third parties for certain elements of the due diligence process, but the ultimate responsibility for knowing the customer rests with the financial institution. Financial institutions should make sure that the third party referring the business is regulated and supervised according to the FATF Recommendations[90].

Assessment:

From a legal perspective, we have found Saudi Arabia to be fully compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 6.17 of the SAMA-AMLCTF adequately addresses the issues raised by the acceptance of introduced business by third parties, in accordance with applicable international standards. Accordingly, we have found Saudi Arabia to be fully compliant with this principle from a legal perspective.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

[90] FATF Recommendation 9 and Basel 35-36. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Principle 50: Special Purpose Legal Vehicles and Trusts

Standard:

Countries should take measures to prevent the use of legal persons and arrangements by money launderers. Information must be obtained and be made available to authorities about beneficial ownership and control persons of such legal entities[91].

Assessment:

From a legal perspective, we have found Saudi Arabia to be partially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 5.1.2 of the SAMA-AMLCTF addresses the issues covered under this principle. However, we do not consider its language to be adequately compliant with this principle, based on the analysis below.

Both FATF and the Basel CP recommend adequate, accurate and timely information on ownership and control of trust, nominee, fiduciary accounts and corporate vehicles that could be used as fronts (PICs, IBCs). As such, identification and KYC is required on the following:

- beneficial owners
- individuals with control of legal persons
- settlors/grantors
- beneficiaries
- trustees
- intermediate layers of ownership
- holders of bearer shares

SAMA 5.1.2, by contrast, provides only for KYC process on the beneficial owners, Power of Attorney holders and Trustees. There is no specific coverage of fiduciary accounts, bearer share companies, and corporate vehicles used for personal asset holding purposes.

Most significantly, there is no requirement for KYC process on the settlor/grantor of a trust, although this individual is the source of the funds.

---

[91] FATF Recommendation 33 and 34 and Basel 31-34. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Monitoring and Reporting Transactions

The risk of money laundering and terrorist financing cannot be effectively reduced without ongoing monitoring of the transactions. Financial and non-financial institutions expose themselves to money laundering risks if they do not have an understanding of their clients' normal and reasonable patterns of transactions consistent with the business activities. If the institutions do not have the means to detect suspicious transactions, including systems (technology), adequate staff and knowledge, it will be extremely difficult to track terrorist funds. The monitoring and reporting of transactions should be tailored for the level of risk of the account, implying a higher level of monitoring for high-risk accounts.

Principle 51: Requirement to Report Suspicious Transactions (including Terrorist Financing)

Standard:

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations, or represent proceeds from criminal activity, hey should be required to report promptly their suspicions to the competent authorities.[92]

Assessment:

From a legal perspective, we have found Saudi Arabia to be compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Both the KSA-AMLL and SAMA's Rules Governing Anti Money Laundering and Combating Terrorist Financing ("SAMA-AMLCTF") adequately provide for this sort of reporting, and consequently we have found compliant with this principle.

Article 7 of the KSA-AMLL requires that all financial and non-financial institutions immediately inform the FIU of suspicious transactions, and prepare a detailed report on the transaction and the parties involved.

Article 25 of the KSA-AMLL relieves owners, managers, representatives and employees of Financial and Non-Financial Institutions from liability for violating confidentiality provisions in the course of obeying the KSA-AMLL, unless they were acting in bad faith to hurt the involved person.

The SAMA-AMLCFT:

- instructs banks to report any reasonable suspicion to the authorities (Article 3.9),
- confirms their obligation to provide relevant details and documents to SAMA (Article 3.11),
- requires all local banks to report suspicious transactions to both the Saudi FIU and to SAMA (Article 4.1),
- directs banks to establish procedures for cooperating with enforcement authorities through an internal Money Laundering Compliance Unit, or MLCU (Article 7),
- charges banks with formulating suspicious transaction reporting (STR) procedures to ensure that employees report suspicious transactions to the MLCU (Article 12), and
- provides that notification of suspected ML/FT cases to the authorities does not conflict with bank secrecy and customer confidentiality regulations (Article 13.2).

Enforcement:

[92] FATF Recommendation 13 and FATF Special Recommendation IV. The full text of the FATF 40 Recommendations on Money Laundering and FATF Special Recommendations on Terrorist Financing are appended to this report in Annex 1 and 2.

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have no evidence that Saudi Arabia has punished banks or other institutions for not reporting suspicious transactions.

Implementation:

It is difficult to tell whether or not the measures allowed for in these laws have been implemented in Saudi Arabia. The FIU to which financial institutions should report has only recently come on line (see Recommendation 26 for further detail).[93] We understand that in the absence of the FIU, SAMA has adopted its responsibilities in this regard, but information on SAMA's activities is lacking. We have been unable to obtain statistics on how many suspicious transaction reports (STRs) are ever filed with SAMA, the nascent FIU, or any other regulatory authority, or on if or how these authorities act on the STRs.

[93] Interview, Senior US Government Official, November 2003.

Principle 52: Monitoring of Unusual Transactions

Standard:

Financial institutions should have intensified monitoring of all complex, large, or unusual transactions that have no apparent economic reason or lawful purpose. An examination of such transactions should be conducted and the findings should be available to authorities. There should be intense monitoring of high-risk accounts.[94]

Assessment:

From a legal perspective, we have found Saudi Arabia to be partially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

There is no provision in the KSA AML Law regulating both financial and non-financial institutions. This is an area of concern, since the AML Law does not require non-financial institutions to monitor unusual transactions. Although financial institutions are covered by SAMA, we could not obtain specific laws and regulations dealing with non-financial institutions.

SAMA Rules Governing AML, 6.2.3 mandates the monitoring of complex, large or unusual transactions. The background and purpose of each transaction should be examined and exceptions should be reported.

Another area of concern is the transaction monitoring threshold. FATF recommends a threshold of USD/EUR 15,000 as the designated threshold for financial transactions carried out in a single operation or in several operations that appear to be linked. SAMA 6.2.1 mandates a much higher threshold for monitoring transactions at SAR 100,000 (USD 26,660) regardless of the level of risk assigned to the account.

SAMA 6.5.2 indicates that a high-risk account should be subject to close monitoring, but it does not specify what close monitoring entails.

Enforcement:

We have no information on the enforcement of this principle.

Implementation:

The implementation this principle has not been determined. Each bank has developed its internal policies, which are safeguarded as proprietary information. There is no public information available regarding the monitoring of transactions by financial institutions.

---

[94] FATF Recommendation 11 and Basel 53, 54. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

The monitoring of transactions is not mandated for non-financial institutions in the laws that were available to us. There is no information available regarding such activity.

"However, as with customer due diligence, we have concerns that a cultural emphasis on privacy may hinder the effective monitoring of individuals' personal wealth transactions."

Principle 53: Transactions with Countries which Insufficiently Apply the FATF Recommendations.

Standard:

Financial Institutions should give special attention to transactions with persons, companies and other financial institutions from countries which insufficiently apply the FATF Recommendations.[95]

Assessment:

From a legal perspective, we have found Saudi Arabia to be compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

FATF recommends that in dealing with persons, including companies and financial institutions, from countries with insufficient application of FATF Recommendations, the financial institutions should:

a) examine the background and purpose of the transactions
b) establish the findings in writing
c) be available to help competent authorities

In addition, countries are required to take appropriate countermeasures if such a non-compliant country continues to insufficiently apply the FATF Recommendations.

SAMA leaves each financial institution to develop its own internal policies to recognize and report suspicious transactions. No specific guidance is given in dealing with these transactions as per sections 12.1 and 12.2 of the SAMA-AMLCFT. Section 11.3, however, recommends extra due diligence for funds transferred from or to NCCT as defined by FATF. Section 6.5.3 recommends rating the customers who have dealings with the NCCTs as High Risk customers. We thus find Saudi Arabia compliant with this principle.

It must be noted, however, that the NCCT list is not comprehensive, as FATF has not yet completed the assessment of all countries. In addition, FATF only assesses the legal and regulatory compliance, not the implementation and enforcement of the regulations.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

---

[95] FATF Recommendation 21. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

Principle 54: Monitoring Currency Transactions

Standard:

Countries should consider:

a. Implementing feasible measures to detect or monitor the physical cross-border transportation of currency and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

b. The feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.[96]

Assessment:

From a legal perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 14 of the KSA-AMLL states that the Implementation Rules will define the regulations and procedures for the amount of cash and precious metals that can be carried in or out of Saudi Arabia and are subject to declaration. These Implementation Rules are not expected to be released until late November 2003, and we have not been able to review them.

We have no KSA Law that purports to detect or monitor the physical cross-border transportation of currency or negotiable instruments.

We have no KSA Law that purports to require financial institutions to report currency transactions above a certain threshold, to a national central agency.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

[96] FATF Recommendation 19. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

No information is available on any Saudi government efforts regulate the flow of cash and precious metals. The Implementation Rules will guide implementation and enforcement. Without them, it is even uncertain which authorities will be responsible for enforcement in this area. It should be noted, thought, that much of the AML-CTF regime's regulatory apparatus can be avoided by physically moving funds in cash. Currency smuggling is common in the Middle East.[97] Border controls are weak and economies are cash-based. Money or readily convertible commodities such as gold or gemstones can be moved using routes and methods commonly employed by criminal organizations.

[97] Greenberg et al. Terrorist Financing: Report of an Independent Task Force Sponsored by the Council on Foreign Relations (2002), 16.

Principle 55: Monitoring of Wire Transfers

Standard:

In order to detect the use of wire transfers for terrorist financing purposes, financial institutions should ensure that accurate and complete information on the originator and the beneficiary of the wire transfer is recorded and included with the wire transfer through the entire chain. Enhanced scrutiny and monitoring of suspicious activity pertaining to funds transfer not containing complete information should be performed.[98]

Assessment:

From a legal perspective, we have found Saudi Arabia to be largely compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

SAMA- AMLCTF, 3.10 requires banks to record and be able to provide the remitter's name, account number, address and the purpose of the remittance for all outgoing transfers. Article 11.1 requires banks to have full information on the remitter's and beneficiary's name, the remitter's address and the account number, and the purpose of the remittance for all incoming and outgoing transfers. Such information should be available upon request.

Neither of the two articles requires enhanced monitoring of the transactions with incomplete information. For this reason, Saudi Arabia is only largely compliant with this principle. Industry business practices recommend the investigation of such occurrences, attempt to collect the missing information, and eventually reporting the suspicious transaction if the information is not available[99].

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

---

[98] FATF Special Recommendation VII. The full text of the FATF Special Recommendations on Terrorist Financing is appended to this report in Annex 2.

[99] Interview with compliance officer at large international bank November, 2003.

Retention of Records

Records of transactions and identification data are necessary documents in order to reconstruct transactions and follow the money trail in an investigation. If such documents are destroyed, not maintained long enough, or are not made available to competent authorities, then the reconstruction of evidence is seriously impaired.

Principle 57: Retention of Records

Standard:

Financial institutions should maintain transaction records and identification data for at least five years. Such records should be readily available to domestic authorities upon request. Industry best practices extend this requirement to non-financial institutions that are involved in financial transactions.[100]

Assessment:

From a legal perspective, we have found Saudi Arabia to be compliant with this principle.

From an implementation and enforcement perspective, Saudi Arabia is compliant in terms of financial institutions but we have not been able to verify compliance in terms of non-financial institutions.

Law:

The KSA AMLL Article 5 goes beyond the recommended 5-year period for retention of records both for financial and non-financial institutions, and mandates a minimum of 10 years retention. The type of documents required to be maintained are "all records and documents that explain the financial, commercial and monetary transactions, the files of commercial accounts and correspondence and copies of the ID".

SAMA-AMLCFT, Article 8 is specific about the documents that should be maintained, but does not specify the retention period for the records under section 8.1, which include records of all customer transactions, account opening documents, customer IDs, and details of customer accounts and balances. Section 8.2 stipulates that certain non-financial documents, including KYC related documents and suspicious activity reports, must be maintained for a period of 10 years.

Saudi Arabia has thus provided for the retention of the appropriate records for an appropriate period. There is some ambiguity, however, in that the KSA-AMLL Article 5 issues a decisive time period over which documents must be preserved, but does not specify precisely which documents. SAMA-AMLCFT, Article 8, which should refine KSA-AMLL Article 5, is specific about documents but in Section 8.1 does not indicate for how long these important documents are to be preserved.

Enforcement:

Saudi Arabia does enforce record-keeping requirements on banks[101]. We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective with regard to non-financial institutions.

---

[100] FATF Recommendation 10: The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.

[101] Interview with former senior SAMBA employee, November 12 2003

Banks are required to maintain records of transactions and Identification documents, including other KYC related documents. It is not clear how long each type of records must be maintained. We could not verify the implementation/enforcement of this principle by non-financial institutions.

Implementation:

Saudi banks have implemented record-keeping requirements.[102] We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective with regard to non-financial institutions.

[102] Interview with former senior SAMBA employee, November 12 2003

Non-Financial Businesses

Non-financial businesses pose a high-risk of Money Laundering and Terrorist Financing due to a less stringent regulatory environment. Of special concern are sectors that involve the transfer of liquid assets on a large scale. Any flow of liquid assets presents the opportunity for money laundering or for the transfer of funds to terrorists. Such non-financial businesses include, but are not limited to, real estate agents, dealers in precious metals and stones, lawyers, notaries and other independent professionals. For similar reasons, alternative or informal remittance systems are another sector of serious concern.

Principle 57: Regulation and Supervision of Non-Financial Businesses

Standard:

Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organization, provided that such an organization can ensure that its members comply with their obligations to combat money laundering and terrorist financing.[103]

Assessment:

From a legal perspective, we have found Saudi Arabia to be largely non-compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL covers "Financial and Non-Financial Institutions," defined in Article 1(5) as any establishment in the kingdom engaged in any one or more financial, commercial or economic activity such as banks, money-exchangers, investment companies, insurance companies, commercial companies, establishments, professional firms or any other similar activities set forth in the Implementation Rules.

The SAMA-AMLCFT addresses itself solely to banks. The Saudi Arabia Monetary Agency Law (the "KSA-SAMA") authorizes SAMA to "control commercial banks and persons engaged in the exchange of currencies business" (Article 1(c)). The KSA-BCL, in Article 1, defines a bank as anyone engaged in any banking business, and defines "banking business" as
operations of receiving monies as current or fixed deposits, the opening of current accounts and credits, the issue of letters of guarantee, payment and collection of cheques, orders, payment vouchers and other documents having value, discount of bills and promissory notes and other commercial papers, foreign exchange business and other banking business.

From the laws to which we have access, SAMA does not appear to have the authority to oversee entities other than banks and money changers, though we understand that SAMA also regulates the insurance sector and the securities market.[104] Yet even using the expansive definition of "banking business" in the KSA-BCL, this still does not cover alternative remittances conduits. We note that SAMA has made efforts to engage these issues by promulgating rules to banks dealing with charitable organizations and hawaladars, but that is still an indirect and unsatisfactory way of achieving oversight of them.

---

[103] FAFT Recommendation 24. The full text of the FATF 40 Recommendations on Money Laundering is appended to this report in Annex 1.
[104] Interview, Senior U.S. Government official, November 21, 2003.

We also note that the KSA-BCL itself appears to place money changers under a separate regime from banks (Article 2(b)), and we have not seen these institutions addressed in any regulatory framework. We understand that SAMA is in charge of regulating money changers, but we have seen no regulations that apply to them.

We stress the need for oversight of cash-intensive non-bank, non-money changer businesses such as precious commodities dealers, pawnbrokers, travel agencies, and import/export businesses, as well as real estate brokers, lawyers and accountants. Regulated record keeping and due diligence that made it possible to link individuals to specific transactions, as well standards for suspicious transactions and protocols for reporting them, would strengthen the Saudi CTF regime.

The AML/CFT regulatory framework functions as an integrated whole. Even if the KSA-AMLL Implementation Rules are extended to all relevant institutions, Saudi enforcement of those rules will be damaged without the type of thorough, rigorous and professional compliance measures that SAMA has promulgated in the banking sector.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 58: Due Diligence Recommendations Applied to Non-Financial Institutions

Standard:

The same level of due diligence performed by financial institutions should apply to non-financial institutions.[105]

Assessment:

From a legal perspective, we have found Saudi Arabia to be largely non-compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Most of the regulations that apply to financial institutions should also apply to Non-Financial Institutions, particularly those NFIs cited by FATF Recommendations 12 and 16. As noted above, the AML/CFT regulatory framework functions as an integrated whole. While the KSA-AMLL applies to NFIs, the SAMA-AMLCFT does not. Even if the KSA-AMLL Implementation Rules *are* extended to all relevant institutions, Saudi enforcement of those rules will be damaged without the type of thorough, rigorous and professional compliance measures that SAMA has promulgated in the banking sector.

We are missing the "Implementation Rules" referenced in the KSA AML. We are also missing any and all relevant regulations imposed by KSA government ministries (esp. the Ministry of Commerce) to address these issues, such as the "Regulations for Companies" or the "Saudi Arabian Auditing Standards."

We have found Saudi Arabia to be only partially compliant with this principle for the following reasons:

a. Ambiguous Scope of the Law

We are concerned with the scope of Saudi law in regard to this principle. The KSA AML Law refers to various forms of Non-Financial Institutions and incorporated entities, companies, establishments, and firms. It is not clear that these categories include proprietorships, precious commodities dealers, or professionals such as lawyers or accountants.

b. Due Diligence

AML 4 covers fictitious names and numbered accounts, but requires verification of a client's identity "at the start of dealing with such client ... *or* upon concluding commercial transactions therewith." [emphasis added] Such timeline stipulation leaves the law vulnerable to exploitation.

It is also vague on verification standards, has no provision for verification of identity upon doubt or suspicion, has no thresholds for closer scrutiny, has no ongoing due diligence, is ambiguous

[105] FATF Recommendation 5, 6, 8-12, 13, 14, 15, & 21 Basel 18,19, 22, 23, 35-36, 41-48, 55-59 and Industry best practices. The full text of the FATF 40 Recommendations on Money Laundering and of the Basel's Customer due Diligence for Banks are appended to this report in Annex 1 and 3.

about verifying the control structure and beneficial ownership in a transaction, is silent on understanding "the intended nature" of the business relationship, and has no requirements for action if verification is not successful

There is no discussion of PEPs in the KSA AML, so there may be no additional due diligence or caution on the part of NFIs in dealings with such individuals. Similarly, there is NO discussion of 3rd-party due diligence in the KSA AML, even though FATF Recommendation 12 suggests that most of the recommended due diligence measures be extended to third-parties with which the NFI has dealings.

c. Record-Keeping

AML 5 covers record-keeping but is ambiguous. It goes beyond the required minimum 5 year period for retention of records both for financial and non-financial institutions, and mandates a minimum of 10 years retention. The type of documents required to be maintained are "all records and documents that explain the financial, commercial and monetary transactions, the files of commercial accounts and correspondence and copies of the ID". The phrase "records and documents that explain the transactions" is ambiguous.

d. Detection and Reporting of Suspicious Transactions

AML 6 & 7, in combination, *might* be construed to cover suspicious transactions, but are extremely vague. Article 6 requires institutions to have in place measures to "detect and foil any of the offences herein." Article 7 follows this with language referring to "complex unusual large or suspicious transactions."

AML 7 requires Non-Financial Institutions to immediately notify the FIU and submit a report regarding suspicious transactions. However, this requirement is preceded by the phrase "upon gathering *sufficient* indications and evidence" [emphasis added], without explanation as to what constitutes "sufficiency" in this case.

e. Provision of Information and Safe Harbour

AML 8 stipulates an obligation to provide documents, records, and information – "subject to confidentiality provisions" and "in accordance with applicable regulations." The secrecy provision, AML 13, provides that "information disclosed by NFI's *may* be shared with the concerned authorities *if* such information is connected with a violation of these Regulations." [emphasis added] It is unclear how forthcoming this actually requires NFIs to be.

There appears to be no safe harbour for NFI employees, though as noted above, AML 13 provides that information may be provided in certain circumstances. There is no explicit protection for those who provide the information.

f. Internal Policies and Procedures

AML 10 requires NFIs to develop internal policies, procedures, and controls, as well as ongoing training programs, and internal audit functions. The law is somewhat vague about training requirements and also does not mention adequate employee screening procedure, and makes no mention of external auditors (as per Basel 59). Otherwise, the law is largely compliant on this issue.

Enforcement:

We have not been able to verify Saudi Arabia's compliance with this principle from an enforcement perspective. We have not been able to obtain the necessary data to make an informed assessment.

Implementation:

We have not been able to verify Saudi Arabia's compliance with this principle from an implementation perspective.

Principle 59: Alternative Remittances

Standard:

Alternative remittance systems should be licensed and subject to the same level of scrutiny that apply to financial and non-financial institutions..[106]

Assessment:

From a legal perspective, we have found Saudi Arabia to be partially compliant with this principle.

From an enforcement and implementation perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Overall, Saudi law is ambiguous, conflicted and incoherent on the issue of alternative remittances such as hawala. The status of the business of alternative remittance is not clear under Saudi law, nor is the status of money changers who may carry out this business. It is unclear what regulations, if any, govern this form of money transfer, though it does appear that SAMA has authority for licensing money changers of all types. However, even SAMA's rules are unclear about the status and legality of alternative remittances.

KSA AML Article 1 defines banks to include all natural or legal person who carry on "banking activities," which includes "receiving money on current or fixed deposit account, opening of current accounts, opening of letters of credit, issuance of letters of guarantee, payment and collection of cheques, payment orders, promissory notes and similar other papers of value, discounting of bills, bills of exchange and other commercial papers, foreign exchange transactions and other banking business." This appears to include part of the money changing business; as noted above in Principle 25, however, it is not clear that this includes alternative remittance conduits.

We also note that the KSA BCL appears to place money changers under a separate regime from banks (Article 2(b)), and KSA Banking Control Law Article 2b limits the business of money changers to the "exchange of currency." However, this appears to conflict with the Regulations for Money Changing Business Article 3b, which stipulates that "the Saudi Arabian Monetary Agency may license any money-changer to make *cash remittances* inside and outside the Kingdom." [Emphasis added.] It is not clear that such money-changers are subject to the SAMA Rules Governing AML, or any other such regulations, since the KSA BCL Article 2b does not appear to recognize such remittances by money changers as "banking business."

We have not seen these institutions addressed in any substantial regulatory framework. We understand that SAMA is in charge of regulating money changers, but other than the Regulations for Money Changing Business, which do not address AMLCTF, we have seen no rules that apply to them. SAMA has no visible directives pertaining to the control of the initial transaction, no

[106] FATF Special Recommendation VI: The full text of the FATF Special Recommendations on Terrorist Financining is appended to this report in Annex 2.

discussion of how to monitor the settling of claims across hawala networks, and no regulations on the methods of practice of hawala. Although this level of detail in the regulation of the hawala system may exist in the KSA, no information regarding these details has been made available. If this level of detail does not exist, then this remains a serious vulnerability of the Saudi financial system to money laundering and terrorist financing, one in which the KSA is well behind other countries in its regulatory establishment.

KSA Banking Control Law Article 2 renders unlicensed *banking* activities to be illegal, and SAMA Rules Governing AML Article 9 defines "unlicensed" or "unauthorized" alternative remittances to be illegal, and movement of funds for such purposes to be considered a "suspicious transaction." However, although "authorized" hawala appears to be legal under the Regulations for Money Changing Business, the SAMA-AMLCFT Article 5.1.8 decrees that banks should not allow accounts that are used for *any* alternative remittances such as hawala, and should report such activity as "Suspicious Activities."[107] [Emphasis added.] As such, SAMA's position on alternative remittances appears inconsistent It should be noted that the Regulations for Money Changing Business, promulgated in 1981, declares a moratorium on new licenses for money changing businesses.

Implementation / Enforcement:

In practice, there are some nine organized "money houses" licensed to carry out remittances, as well as some number of licensed "money-changers" who are *not* permitted to carry out remittances. To our knowledge, therefore, there are no licensed individual hawaladars, and as such there should *be* no individual hawaladars, and no new exchange houses or individual money changers should have opened for business since 1981.

Informal funds transfer systems such as hawala are a major element of wealth movement in and out of the Kingdom of Saudi Arabia, and may well be the largest method by which money enters and leaves the KSA. There are multiple forms of hawala, including single-hawaladar operations (where the individual or entity has multiple international bank accounts) and hawaladar-network (where multiple individuals or entities operate across an international network) operations. Each has its own vulnerabilities to exploitation by money-launderers and terrorism financiers, and each poses different challenges to regulators.

We have been unable to verify the enforcement of the licensing restrictions, which have been in place since at least 1981. Data on unlicences remittances is notoriously difficult to acquire. However, it appears that the Saudi government has not succeeded in fully regulating alternative remittances, judging by the continued existence of hawaladars outside the licensed exchange houses.[108] It is also unclear how the money changing business has sustained itself in the 23 years since the Regulations for Money Changing Business required SAMA to stop issuing licenses for money changers.

SAMA, in the May 2003 rules for AMLCTF, has made suggestions to banks on how to identify hawaladars of the first variety (single-entity, multiple-account operations). However, since the main financial transfer mechanism of these operations lies outside the KSA, this measure may be largely ineffective if it is not accompanied by a coordination of efforts between Saudi Arabia and

[107] SAMA, *Rules Governing Anti Money Laundering and Combating Terrorist Financing*, May 2003, Article 5.1.8.
[108] Interview with Sheikh Hamad Al-Sayari (governor of SAMA), "Strength to strength," *The Banker*, October 2002.

other countries to control and monitor inter-account transfers. Given the tight control and overall opacity and secrecy that permeates the Saudi financial sector, there is reason to question the extent to which this level of international coordination can occur. With respect to the second variety of hawala, the multiple-intermediary form, there appears to be no discussion of how to address this type of operation.

Conclusion – Regulatory Regime

Our review and analysis of Saudi Arabia's AML-CFT Regulatory Regime has highlighted a number of areas in which that system is fully or substantially compliant with relevant international standards. Saudi Arabia has made important strides in creating an effective infrastructure for combating money laundering and terrorist financing, including enacting legislation, establishing supervisory, reporting and enforcing bodies, and mandating the creation of efficient internal policies and procedures for financial and non financial institutions. The laws and regulations dealing with customer due diligence, transaction monitoring, and retention of records are largely adequate. However, there are also several issues of concern, which will require continuing attention:

1. The Regulatory Infrastructure may not be effectively implemented. Saudi Arabia's secrecy laws may impede the full implementation of the International Standards and industry best practices in the areas of collaboration between regulatory and enforcement bodies and international cooperation. There is no reliable information regarding the country's financial and human resources in regulatory and enforcement capacity, including the level of training of employees of financial and non-financial institutions, law enforcement agencies and regulatory bodies. There are no provisions in the law for the screening of employees in order to ensure the highest standards of moral conduct of the employees in critical positions with respect to money laundering and terrorist financing. The level of implementation of AML and CTF policies in foreign branches and subsidiaries might not be the same as the standard established in Saudi Arabia. In addition, there is concern regarding the functionality of the newly created FIU and its role in effectively analyzing suspicious activity reported by financial and non-financial institutions.

2. The customer due diligence might be inadequate with respect to certain categories of customers. We are missing SAMA circulars and Implementation Rules dealing with customer identification and due diligence, therefore we could not fully assess the compliance with the standards. The provisions of the laws dealing with Politically Exposed Persons do not specifically cover the royal family, and do not require an evaluation of the source of wealth. The laws also lack due diligence elements with respect to Correspondent Banking, and are inadequate with respect to special purpose vehicles and trusts.

3. Due to Saudi Arabia's lack of transparency, the implementation and enforcement of transaction monitoring cannot be reasonably assessed. The FIU is not fully functional. We do not know if it is able to process and act on reported suspicious transactions. We have no information about the monitoring of transactions by non-financial institutions. We have no information regarding the monitoring of cash transactions. The threshold for monitoring transactions is higher that industry best practices and FATF recommendations (USD 26,660 versus USD 15,000). The procedures and standards for enhanced monitoring of unusual transactions or transactions with incomplete information are not clear or are not available. Transactions with countries with lax AML controls are not subject to enhanced scrutiny, except for the NCCT countries.

4. The regulation and supervision of non financial businesses may be substantially inadequate. Other than the largely inadequate KSA-AMLL, we were unable to obtain any significant legislation dealing with AML-CTF in non financial business sectors. We also could not obtain significant information regarding the implementation and enforcement of the AML and CTF regulations. Some of the legislation dealing with non financial businesses and alternative remittance systems is new, and the implementation and enforcement may not have been fully completed as yet. Particularly with respect to alternative remittance systems, the laws we were able to obtain are unclear, contradictory, and in need of substantial revision and clarification.

Non-Profit Sector (Charities)

To assess the effectiveness of Saudi Arabia's regulations in combating terrorist financing through charities, we have performed a step-by-step comparison of Saudi Arabia's laws with the international best practices outlined by the FATF memo "Combating the Abuse of Non-Profit Organizations," issued October 11, 2002. These best practices are broadly divided into four areas of focus, which include financial transparency, programmatic verification and administrative and oversight bodies. We will examine Saudi Arabia's regulatory regime in each of these areas.

Financial Transparency

Financial transparency guarantees that charitable organizations maintain documentation that accounts for all their programs. To insure the transparency of charitable operations, independent auditing is an efficient and widely recognized method of ensuring that accounts of an organization accurately reflect the reality of its finances.

1. Principle 60: Financial Accounting Transparency

Standard:

Non-profit organizations should maintain and be able to present full program budgets that account for all program expenses. These budgets should indicate the identity of recipients and how the money is to be used. The best practices do differentiate between administrative and program budgets and require both to be protected from diversion.[1]

Assessment:

From a legal perspective, the relevant Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, we have not been able to verify Saudi Arabia's compliance with this principle.

Law:

Article 11 of the 1981 Regulations Regarding Charities requires all charities to "keep a record of all financial statements, budgets, and money raised, its sources and how it is spent."[2]

Enforcement / Implementation:

Saudi Arabia's regulations in this area meet the standards outlined by the FATF. In some respects, Saudi Arabia's regulations go further than international best practices. By requiring charities to keep a record of their budgets and expenses and consolidate all of their accounts into a single account that is strictly controlled, the Saudi Arabia's regulatory regime provides a mechanism for authorities to monitor the finances of charities.

---

[1] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[2] *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

Principle 61: Independent Auditing

Standard:

Independent auditing is a widely recognized method of ensuring that accounts of an organization accurately reflect the reality of its finances and should be considered a best practice. Where practical, such audits should be conducted to ensure that such organizations are not being used by terrorist groups. It should be noted that such financial auditing is not a guarantee that program funds are actually reaching the intended beneficiaries.[3]

Assessment:

From a legal perspective, the relevant Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

According to Article 16 of the 1981 Regulations Regarding Charities, the MLSA has "the right to review all files and registers. If an MLSA officer presents himself and requests information about the association, the association must provide this officer with such information."[4]

Enforcement / Implementation:

A large loophole with regards to the financial accounts of charities is the lack of regular and independent audits. Though the 1981 Regulations Regarding Charities states that the MLSA has "the right to review all files and registers," it does not require any regular inspections. Also, an audit performed by a MLSA officer would not be considered truly "independent" since the MLSA is the regulatory body for all charities in Saudi Arabia.

In the Green Book and other recent reports, Saudi Arabia has claimed that it has performed full audits of all its charities – "Since September 11, all charitable groups have been audited to assure that there are no links to suspected groups."[5] However information about these audits has not been made public. It is not clear who performed the audits, what standards were used and what the specific results were. Also, these reviews may not have examined the foreign operations of Saudi Arabian charities.

---

[3] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[4] *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

[5] *Initiatives and Actions in the Fight Against Terrorism*, The Kingdom of Saudi Arabia, Summary Report, September 2003

Principle 62: Registered Bank Accounts

Standard:

It is considered a best practice for non-profit organizations that handle funds to maintain registered bank accounts, keep its funds in them, and utilize formal or registered financial channels for transferring funds, especially overseas.[6]

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

The new SAMA regulations passed in May of 2003 require banks and money-changers to require depositors to provide them with identification and other required information for verification before accepting deposits from charities. In addition," all bank accounts of charitable or welfare societies must be consolidated into a single account for each such society."[7] Going beyond the international standards, Saudi Arabia has banned its charities from transferring any funds abroad and requires charities to receive permission from SAMA to open a bank account. In addition, new regulations place strict controls of the bank account of charities, preventing such transactions as cash withdrawals and credit card usage.

Enforcement / Implementation:

One potential loophole is the hawaladars or money changers who often operate with little regulatory oversight in Saudi Arabia. Though they technically fall under the jurisdiction of SAMA, according to one expert on the Saudi Arabia's financial sector, it has proven difficult for the authority to exert control over the network of money changers that dot the country.[8] Many do have the required licenses but many of these hawaladars do not keep detailed records and do not have the internal controls of a bank. Thus, it appears to remain relatively easy for a charitable organization within Saudi Arabia to open up an account with a money changer without the permission of SAMA and transfer funds under the radar of the monetary authority.

Another weakness of the new regulations is the lack of oversight over individuals who may be funneling funds to terrorist organizations abroad. Some experts have argued that individuals, not charities, are the largest contributors to terrorist organizations like Al Qaeda. **Brisard,** for instance, noted that the Golden Chain list found in the offices of Benevolence International Foundation, a charity operating in Sarajevo, was composed of the top 20 Saudi financial sponsors of Al Qaeda. All of them were individuals and they had a cumulative net worth of $85 billion or 42% of the Saudi annual GNP.[9] The new regulations do not put a stop to the flow of funds from wealthy individuals like these, who can still easily open up bank accounts and make transfers abroad.

---

[6] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[7] Saudi Information Office, Press release, June 12, 2003

[8] Interview with Saudi banking expert November 2003

[9] Jean-Charles Brisard testimony to the Committee on banking, housing and urban affairs U.S. Senate October 22 2003

Also, since Saudi Arabia has no capital controls, any charity, group or individual could simply carry an unlimited amount of cash out of the country. In fact, the practice of physically moving cash abroad is so well-established in Saudi Arabia that there are courier services that specialize in cash deliveries to international financial centers like Dubai.

Finally, it appears that it remains possible for individuals who seek to donate to illegitimate organizations with charity fronts abroad to transfer funds abroad through their own accounts or by creating new ones, both in Saudi Arabia and abroad. In addition, even with new regulations placing strict controls on charitable funds, Saudi Arabian charities outside of the country have continued to operate, raising the question of how this is possible.

Programmatic Verification

Programmatic verifications encompass the solicitation of information regarding the donors and the beneficiaries of charitable donations. These verifications should be implemented periodically by transparent and credible authorities to insure the application of best practices and the non misuse of charitable organizations domestically and abroad.

Principle 63: Transparent Solicitation

Standard:

Solicitations for donations should accurately and transparently tell donors the purpose(s) for which donations are being collected. The non-profit organization should then ensure that such funds are used for the purpose stated.[10]

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no regulations regarding the solicitation of donations in the Kingdom. However, in May of 2003, the Ministry of Labor and Social Affairs banned all donation-boxes in mosques.

Enforcement / Implementation:

Donation boxes have been a particular problem in Saudi Arabia in terms of combating terrorist financing. Funds collected in donation boxes are distributed by mosques to various individuals and groups with little oversight of these distributions.

In recent months, during investigations into the Riyadh bombings, a clear link was indentified between these donation boxes and Al-Qaeda. The *Jedda Arab News* reported on September 17th, "in raids on a small farm and a rest house in Riyadh as well as locations in Qasim and the Eastern province, security forces seized rocket-propelled grenades, explosives and detonators as well as night- vision binoculars, monitoring cameras, computers, fake passports and ID cards and *collection boxes*."[11]

Consequently, Saudi Arabia has moved to curtail *zakat* through donation boxes. An article in the *Jedda Arab News* quoted Interior Minister Prince Naif as warning "people to be wary of putting money in collection boxes found at the entrance to some mosques. 'Those wishing to contribute must verify where the money will go,' he said. He urged Saudi citizens, 'not to contribute unknowingly to the killing of people by paying money to suspicious boxes or parties.'"[12] And in August of this year, the Ministry of Labor and Social Affairs banned the collection of cash through donation boxes placed in mosques, schools and shopping malls. However, Western experts on Saudi Arabia have recently reported that even after the ban, these boxes continue to be placed in mosques and other areas.[13]

---

[10] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002
[11] The *Jedda Arab News* article 17 September 2003
[12] The *Jedda Arab News* article 17 September 2003
[13] Interview with Saudi banking expert November 2003

Some experts have pointed out that Saudi Arabia has made several previous attempts to regulate its charities – to no avail. Brisard testified that there have been many regulations including the 1976 Fundraising for Charitable Purposes Regulation and the 1994 royal decree banning the collection of money in the Kingdom for charitable causes without official permission. But he noted, "through these various unsuccessful attempts to regulate or control the recipients of *zakat* or donations, one must question the real ability and willingness of the Kingdom to exercise any control over the use of religious money in and outside the country." [14]

[14] Jean-Charles Brisard testimony to the Committee on Banking, Housing and Urban Affairs U.S. Senate October 22, 2003

Principle 64: Programmatic Oversight

Standard:

To help ensure that funds are reaching the intended beneficiary, non-profit organizations should ask the following general questions:

Have projects actually been carried out?
Are the beneficiaries real?
Have the intended beneficiaries received the funds that were sent for them?
Are all funds, assets, and premises accounted for? [15]

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no Saudi regulations requiring charities to report on whether projects have been carried out, whether the beneficiaries are real and whether they received the funds that were sent to them. However, the 1981 regulations do require charities to keep records of all of their correspondence, their funds and financial statements and requires charities to send the minutes of all of their meetings to the MLSA within 10 days of the meeting (Article 8d). [16]

Enforcement / Implementation:

This is the point of greatest weakness in Saudi Arabia's anti-terrorist financing regulatory regime. By and large, Saudi Arabian regulations regarding programmatic verification do not meet the standards outlined by FATF. These standards require charities to declare the purpose of all solicitations and ensure that the funds are used exclusively for the stated causes and by the groups for which the funds were donated. There are currently no Saudi Arabian laws addressing solicitations in the kingdom and little oversight of how donated funds are used by the charities. Though the 1981 Regulations do require charities to keep records of all of their correspondences, funds and financial statements, they does not specifically oblige charities to account for all of the funds they raise and whether projects are really carried out.

Complicating the issue of donations in Saudi Arabia is the practice of *zakat*. As mentioned above, *zakat* is a requirement for all financially-able Muslims and can be donated in many forms – to the charities or the needy themselves, through the government which collects a *zakat* tax or until they were banned, through donation boxes in mosques and other areas. Anonymous donations are considered particularly pious and those giving *zakat* are usually not interested in how their donations are spent. They are simply interested in the act of giving *zakat*, which meets the religious requirement. Thus, charities and others receiving donations in Saudi Arabia have traditionally had little accountability to their financial backers, including the government.

---

[15] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[16] *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

Zakat taxes are collected and controlled by the Department of Zakat and Income taxes (Directorate General of Zakat & Income Tax (DZIT)) of the Saudi Ministry of Finance and National Economy. [17] These donations usually take the form of bank transfers to the more than 240 charities. Though the department has strict instructions for organizing, auditing, and collecting *zakat* from all Saudis obligated to pay, it has had little guidance on how these funds should be distributed. Also, there are no regulations regarding the oversight of these funds once they are received by the charities. Thus, charities in the kingdom have been and are still receiving billions of dollars from the government without public accountability of where these funds are going.

[17] http://www.mof.gov.sa/e_alzakah.html

Principle 65: Field Auditing

Standard:

Direct field audits of programs may be, in some instances, the only method for detecting misdirection of funds. Examination of field operations is clearly a superior mechanism for discovering malfeasance of all kinds, including diversion of funds to terrorists. However, non-profit organizations should track program accomplishments as well as finances. Where warranted, examinations to verify reports should be conducted. [18]

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no regulations requiring field audits for charities in Saudi Arabia. However, as mentioned above, the MLSA has the right to demand and review all the files and registers of charities.

Enforcement / Implementation:

A large loophole with regards to the financial accounts of charities is the lack of regular and independent audits. Though the 1981 Regulations Regarding Charities states that the MLSA has "the right to review all files and registers," it does not require any regular inspections. Also, an audit performed by a MLSA officer would not be considered truly "independent" since the MLSA is the regulatory body for all charities in Saudi Arabia.

In the Green Book and other recent reports, Saudi Arabia has claimed that it has performed full audits of all its charities – "Since September 11, all charitable groups have been audited to assure that there are no links to suspected groups."[19] However information about these audits has not been made public. It is not clear who performed the audits, what standards were used and what the specific results were. Also, these reviews may not have examined the foreign operations of Saudi Arabian charities.

---

[18] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[19] *Initiatives and Actions in the Fight Against Terrorism,* The Kingdom of Saudi Arabia, Summary Report, September 2003

Principle 66: Foreign Operation Oversight

Standard:

Where possible, a non-profit organization should take appropriate measures to account for funds and services delivered in locations other than in its home jurisdiction.[20]

Assessment:

From a legal perspective, Saudi Arabia is partially in compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

There are no specific laws or regulations that empower the government of Saudi Arabia to oversee the operations of its charities outside of the country. However, the 1981 Regulations state "charities cannot open subsidiaries without the permission of the MLSA." In addition, the SAMA regulations issued in May of this year do allow the government to control how much money domestic Saudi charities are sending abroad.[21]

Enforcement / Implementation:

The new regulations restrict charities from transferring any funds abroad without authorization from SAMA. This is another key regulatory issue for Saudi Arabia. Its charities' foreign operations are wide-ranging and have often been accused as serving as the points of delivery of funds to terrorist organizations. For instance, the Saudi-supported World Assembly of Muslim Youth operates in 55 countries while the International Islamic Relief Organization, another organization backed by Saudis, is reputed to have offices in over 90 countries. Both have been charged in the media with "passing on money" to terrorist organizations.[22] Both deny involvement and cite a large number of legitimate charitable projects.

Though limited, Saudi regulations of charities' foreign operations go further than FATF recommendations, which only state that "the competent authorities in both jurisdictions should strive to exchange information and co-ordinate oversight or investigative work." The 1981 Regulations require charities to get permission from the MLSA before opening any subsidiaries. However, this area remains a vague in terms of legal authority and enforcement.

---

[20] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[21] *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

[22] Interview with Saudi banking expert November 2003

Principle 67: International Cooperation

Standard:

When the home office of the non-profit organization is in one country and the beneficent operations take place in another, the competent authorities of both jurisdictions should strive to exchange information and co-ordinate oversight or investigative work, in accordance with their comparative advantages.[23]

Assessment:

From a legal perspective, Saudi Arabia is non-compliant.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

We found no specific law relating to this matter. However, according to a Saudi Embassy press release on October 18, 2002, Saudi Arabia and the U.S. maintain a counter-terrorism committee comprised of intelligence and law enforcement personnel who meet regularly to share information and plan actions to curb terrorism financing.[23]

Enforcement / Implementation:

Information sharing among government agencies is critical to the efforts to tackle terrorism financing. The global aspect of many terrorist groups is imposing a new reality on government agencies: the need for further international cooperation. Al-Qaeda is a stunning example of a terrorist group able to plan and coordinate its operations worldwide efficiently. While much of the information collected by single government agencies can be of significant value in terrorism financing investigations, the value will not be realized nor maximized absent the ability to share it with other agencies worldwide.

The establishment of the U.S- Saudi Joint Task Force in the wake of the terrorist bombings in Riyadh on May 12, 2003 is an important step toward further international cooperation between the U.S. and Saudi agencies. Through this initiative, the FBI and the Internal Revenue Service (IRS) have officials stationed in Saudi Arabia to search individuals and charities bank accounts and computer records for links to terrorism. This is also an opportunity to join linguistic, computer, and forensic talents in the fight against terrorism.[25]

Because of these uncertainties, it is crucial to increase cooperation between U.S. and Saudi agencies in charge of monitoring charities to track their finances and their uses both in Saudi Arabia and abroad. In addition, better coordination in the Joint Task Force can help make up for some deficiencies in the current oversight of charities. On October 2003, Saudi officials unveiled what it called a new manual on the charities regulation, which in large part was based on the Charities

---

[23] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[23] Saudi Embassy in Washington Press release October 18, 2002

[25] Saudi Embassy in Washington, Press release, August 26, 2003

Regulation Act of 1981. In both cases, the issue of whose responsibility it is to oversee Saudi charities operating abroad is not clear. This leaves a major gap between theory and reality that can be filled through U.S- Saudi cooperation.

In addition to sharing information regarding charities operating in KSA, Saudi authorities could also provide their U.S. counterparts with information related to Saudi charities established in the U.S. This would greatly benefit ongoing investigations by U.S. agencies into Saudi charities operating in the U.S. One example where cooperation would have been crucial involved the Saudi charity International Islamic Relief Organization (IIRO) based in the U.S. under the name International Relief Organization (IRO.) The IIRO was part of an FBI investigation that unraveled a series of Saudi-sponsored charities in Northern Virginia that are linked to Al-Qaeda and its offshoots.[26]

According to an affidavit filed by the Bureau of Immigration and Customs Enforcement, the IRO invested $3.7 million in BMI Inc. a private Islamic investment company established in New Jersey that may have passed the money on to terrorist groups. The affidavit contends that the IRO originally received $10 million from Saudi Arabia in 1991. The money was then used to set up a shell company called Sana-Bell, Inc which was responsible for investing it. According to the affidavit, between 1992 and 1998 Sana-Bell gave $3.7 million to BMI. A few years later the funds invested in BMI disappeared. The case of IRO is a classic example of how there is a need for enhanced U.S. Saudi cooperation and how that can benefit such investigations.[27]

International cooperation between U.S and Saudi agencies have produced some concrete results, including freezing the accounts of the Al-Haramain Islamic Foundation and shutting down its branches in Bosnia and Somalia in March 2002. While the Saudi headquarters for this private charitable entity is dedicated to promoting Islamic teachings, U.S and Saudi agencies determined that those specific branches of Al-Haramain were engaged in supporting terrorist activities and terrorist organizations such as Al-Qaeda, AIAI (al-Itihaad al-Islamiya), and others.[28]

The United States and Saudi Arabia have also jointly taken action to freeze the assets of a Saudi citizen who headed an organization allegedly giving financial support to Al-Qaeda. In September 2002, the U.S. and Saudi Arabia designated Wa'el Hamza Julaidan, director of the Rabita Trust and other organizations, as a person who supports terrorism.[29]

---

[26] Emerson, Steven and Levin Jonathan, Testimony before the U.S. Senate Committee on Governmental Affairs, July 31, 2003

[27] Farah, Douglas, Terrorist funding affidavit, The Washington Post, August 20, 2003

[28] U.S. Department of State press release, March 11, 2002

[29] U.S. Department of State press release, September 6, 2002

Administration

The transparent administration of the day to day operations of charities and the accountability of their management should be a top priority of charities' oversight agencies. The charities' Board of Directors and employees should act with diligence and probity in carrying out their duties.

Principle 68: Administrative Documentation

Standard:

Non-profit organizations should be able to document their administrative, managerial, and policy control over their operations. The role of the Board of Directors, or its equivalent, is key.[30]

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

The 1981 Regulations require charities to "announce the names of the board of directors and the organizational chart" (Article 1f). The organizational chart should include, among other information required by Article 5, the goals of the charity, the budget and allocation of finances, information about subsidiaries such as their mission and their relationship with the parent charity. Thus, such information would be sufficient to document the administrative, managerial and policies of the charities' operations. In addition, charities must report all changes to the organizational chart, which must be forwarded to the MLSA for authorization (Article 3b). [31]

Enforcement / Implementation:

With regards to laws regulating the administrative operations of charities, Saudi Arabia is mostly in compliance with the international standards set by FATF. The 1981 Regulations require charities to document their organizational charts, their board of directors and goes so far as to require that minutes of all meetings be submitted to the MLSA.

[30] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[31] *Regulations Regarding Associations and Charitable Institutions*, The Kingdom of Saudi Arabia dated 1981

Principle 69: Charity Leadership Accountability

Standard:

The directors or those exercising ultimate control over a non-profit organization need to know who is acting in the organization's name – in particular, responsible parties such as office directors, plenipotentiaries, those with signing authority and fiduciaries. Directors should exercise care, taking proactive verification measures whenever feasible, to ensure their partner organizations and those to which they provide funding, services, or material support, are not being penetrated or manipulated by terrorists.[32]

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

As stated above, charities are required by the 1981 Regulations to announce the names of its board and founding members.

Enforcement / Implementation:

Documentation of charity leadership is required and full. However there are no regulations Regarding the activities of a charity's partner organizations.

[32] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002.

Principle 70: Charity Leadership Responsibility

Standard:

Directors should act with diligence and probity in carrying out their duties. To this end, directors Have responsibilities to the organization and its members to ensure the financial health of the Organization and that it focuses on its stated mandate. Directors are also responsible for those with whom the organization interacts, like donors, clients, suppliers and all levels of government that in any way regulate the organization.

These responsibilities take on new meaning in light of the potential abuse of non-for-profit organizations for terrorist financing. If a non-profit organization has a board of directors, the board of directors should:

Be able to identify positively each board and executive member
Meet on a regular basis, keep records of the decisions taken at these meetings and through these meetings
Formalize the manner in which elections to the board are conducted as well as the manner in which a director can be removed
Ensure that there is an annual independent review of the finances and accounts of the organization
Ensure that there are appropriate financial controls over program spending, including programs undertaken through agreements with other organizations;
Ensure an appropriate balance between spending on direct program delivery and administration;
Ensure that procedures are put in place to prevent the use of the organization's facilities or assets to support or condone terrorist activities.[33]

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

Charities are required by the 1981 Regulations to announce the names of its board and founding members. In addition, the 1981 Regulations require charities to keep records of all of their correspondences, the minutes of all of their meetings and all of their financial transactions (Article 11). As for the board, the 1981 Regulations set out strict standards on various aspects of the board of directors- election must be held by secret ballot, board of directors have 4 year term limits, 90 days prior to election, the MLSA must receive a list of candidates (Article 8).

Enforcement / Implementation:

There are no requirements for annual independent reviews, financial controls, nor for an appropriate balance between spending on direct programs and administration. Most important, neither in the

[33] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002.

1981 Regulations or the SAMA regulations issued earlier this year, are there requirements for procedures that prevent the charity from being manipulated for terrorist financing.

Oversight Bodies

Authorities should have a clear strategy in supervising charities and overseeing their operations. Since many agencies are involved in the oversight practice, there is a need for separation of roles and duties to insure that the control and supervision are implemented in an efficient and professional way.

Principle 71: Law Enforcement Involvement

Standard:

Law enforcement and security officials should continue to play a key role in the combat against the abuse of non-profit organizations by terrorist groups, including by continuing their ongoing activities with regard to non-profit organizations. [34]

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law:

Saudi Arabia has set up a Financial Intelligence Unit that is working to combat against the abuse of charities by terrorist groups. In addition, Saudi secret police and the Money Laundering Section of the Drug Control Office have for many years had oversight of money laundering and other suspicious financial transactions in the country.

Enforcement / Implementation:

As discussed above, by and large, Saudi Arabia has most of the regulations in place to properly combat the abuse of charities for terrorist financing. The question remains how all of these different circulars, royal decrees and ministry regulations will work together, which ministry or authority ultimately has jurisdiction over charities and whether all of these regulations are implemented properly.

[34] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Principle 72: Specialized Government Regulatory Bodies

Standard:

In all cases, there should be interagency outreach and discussion within governments on the issue of terrorist financing – especially between those agencies that have traditionally dealt with terrorism and regulatory bodies that may not be aware of the terrorist financing risk to non-profit organizations. Specifically, terrorist financing experts should work with non-profit organization oversight authorities to raise awareness of the problem, and they should alert these authorities to the specific characteristics of terrorist financing.[35]

Assessment:

From a legal perspective, Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law: It is not clear whether there has been much interagency outreach and discussion within the government on the issue of terrorist financing. There are no regulations calling for cooperation among the many government agencies that oversee the non-profit sector – the MLSA, the Ministry of Islamic Affairs, the FIU, the High Commission, etc.

Enforcement / Implementation:

There is no centralized authority overseeing charities –the Ministry of Labor and Social Affairs, the Ministry of Interior, the Ministry of Islamic Affairs and SAMA each appear to have their own regulations regarding charities. For example, the Ministry of Labor and Social Affairs supervises charity associations but each charity is also required to have audit committees that must answer to the Ministry of Islamic Affairs.

Although the 1981 Regulations clearly state that the MLSA has jurisdiction over charities, the website of the MLSA contains no information at all regarding charities. In addition, recent Saudi press releases cited the Interior Ministry as the agency dealing with charitable organizations. And through the anti-money laundering regulations passed earlier this year, SAMA also has jurisdiction over the charities through their financial accounts.

The discrepancies in the number of registered charities illustrate the disorganization of the MLSA. According to the Kingdom's Charities Report issued by the Saudi government on April 21, 2002, there are 232 registered charities in the Kingdom but the MLSA simultaneously maintains other documents stating that there are only 194.registered charities (see annex). [36]

A further complication is the foreign subsidiaries of Saudi charities. Jurisdiction over these operations is ambiguous. It is not clear if the subsidiaries of Saudi Arabian charities operating outside of the Kingdom are subject to the regulations enforced on domestic operations. The terms "foreign" or "domestic" are not mentioned at all in most Saudi regulations and the Green Book mentions that the Ministry of Foreign Affairs (MFA) is involved in the oversight of Saudi charitable operations abroad. Yet questions remain on how the Ministry specifically monitors these operations,

[35] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[36] *Kingdom's Charities Report* issued by the Saudi government on April 21, 2002

under what regulatory framework and whether it has any jurisdiction over operations that are taking place outside of their territory.

According to a current US government official, the Ministry of Islamic Affairs authorizes the activities of Saudi Arabian charities overseas.[37] The official claims that before opening offices overseas, Saudi charities are required to receive permission from the Ministry of Islamic Affairs. In our research we could not find any documentation about Ministry of Islamic Affairs duties in regards to charities. We were not able to access the website for the Ministry of Islamic affairs, Islam.org.sa, due to the website being password protected. This was the only Saudi government website we found to be password protected. There may not be a contradiction between Ministry of Foreign Affairs foreign oversight and Ministry of Islamic Affairs oversight; however, the lack of any public legislation, the lack of clear mandates to charities to register foreign programming (as opposed to foreign office existence) and the lack of clear institutional authority structures suggest that this is an area of oversight that remains in need of improvement.

FATF suggests that "there should be interagency outreach and discussion within governments on the issue of terrorist financing" (p. 5). At the moment, there doesn't seem to be much outreach or coordination among all the government agencies involved in the regulation of charities in the Kingdom.

The High Commission with oversight of charities was created earlier this year. As the Green Book states, "Saudi Arabia has established a High Commission for Oversight of all Charities(HCOC), contributions and donations.[38] In addition, it has established operational procedures to manage and audit contributions and donations to and from the charities, including their work abroad." But it is not yet clear what role this new body will actually play and how it will interact with the other ministries. Will it be a clearinghouse for all of the regulations? Or will it simply be yet another government body

There is a crucial role for the HCOC to play. A central body is badly needed to coordinate efforts to regulate charities. There is also a need to increase the transparency of the regulatory process; improve the system for appealing decisions made by regulators; and introduce a range of penalties for non-compliance with legal requirements. A thorough preventive regime would also ensure that charities are satisfying their legal obligations and operating for charity purposes. It is unclear whether this task is being done.

---

[37] Interview with current U.S. government official November 2003

[38] *Initiatives and Actions in the Fight Against Terrorism,* The Kingdom of Saudi Arabia, Summary Report, September 2003

Principle 73: Government Bank, Tax, and Financial Regulatory Authorities

Standard:

While bank regulators are not usually engaged in the oversight of non-profit organizations, the current political environment underscores the benefit of enlisting the established powers of the bank regulatory system – suspicious activity reporting, know-your-customer (KYC) rules, etc – in the fight against terrorist abuse or exploitation of non-profit organizations.[39]

Assessment:

From a legal perspective, Saudi Arabia is in full compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law: Part of the anti-money laundering regulations SAMA issued in May of 2003 specifically target charities and through these regulations, the monetary authority does have significant oversight of non-profit organizations within Saudi Arabia. Thus, these regulations not only meet, but in some areas, even go beyond, the international best practices

Enforcement / Implementation:

See Enforcement / Implementation of Oversight Principle 13.

The MLSA charities list supplied in the annex of this report makes clear that more than 70% of Saudi charities deposit their funds at the Al Rajhi Bank, a Saudi Islamic bank. Most Saudi charities are based upon religious principles and so might be expected to choose to process their financial operations through an Islamic bank. Al Rajhi Bank is now being investigated for possibly supporting Osama bin Laden and his Al-Qaeda terrorist network[40]. Though the special relationship between Saudi charities and the Al Rajhi Bank raises questions regarding the potential role that Islamic financial institutions in Saudi Arabia play in terrorism financing, it also provides bank regulators an opportunity to oversee the collection and disbursement of a significant percentage of Saudi Arabia's charitable funds

[39] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002
[40] The Atlanta Journal-Constitution, Nov 16th, 2003

Principle 73: Tax Authority Participation

Standard:

In those jurisdictions that provide tax benefits to charities, tax authorities have a high level of interaction with the charitable community. This expertise is of special importance to the fight against terrorist finance, since it tends to focus on the financial workings of charities.[41]

Law: Saudi Arabia does not tax its charities, thus it would not be able to implement this best practice.

Enforcement / Implementation:

This standard is not applicable to Saudi Arabia.

[41] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Principle 74: Information Sharing

Standard:

Jurisdictions which collect financial information on charities for the purposes of tax deductions should encourage the sharing of such information with government bodies involved in the combating of terrorism (including FIUs) to the maximum extent possible. Though such tax-related information may be sensitive, authorities should ensure that information relevant to the misuse of non-profit organizations by terrorist groups or supporters is shared as appropriate.[42]

Assessment:

From a legal perspective, this is not applicable.

From an implementation/enforcement perspective, this is not applicable.

Law:

Since Saudi Arabia does not tax its charities, it would not be able to implement this best practice.

Enforcement / Implementation:

This standard is not applicable to Saudi Arabia.

[42] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Principle 75: Private Sector Watchdog Organizations

Standard:

In the countries and jurisdictions where they exist, the private sector watchdog or accreditation organizations are a unique resource that should be a focal point of international efforts to combat the abuse of non-profit organizations by terrorists. Jurisdictions should make every effort to reach out and engage such watchdog and accreditation organizations in their attempt to put best practices into place for combating the misuse of non-profit organizations.[43]

Assessment:

From a legal perspective, Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is partially in compliance.

Law: In Saudi Arabia, the MLSA acts as the non-profit sector's watchdog and accreditation organization.

Enforcement / Implementation:

There are few private-sector organizations that have the capacity or knowledge of best practices for combating the misuse of non-profit organizations.

Oversight Bodies Conclusion: In theory, there appear to be many government agencies in charge of regulating and supervising charities. In reality, the role of these agencies is unclear and sometimes, there is overlap which creates bottle necks and major bureaucratic delays.

[43] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

Sanctions

Sanctions are coercive actions taken by the oversight agencies to insure that the regulation in place is well respected. A battery of sanctions ranging from simple financial fines and penalties to imprisonment should allow the charities' oversight agency to conduct its mission and deter any action that is contradictory with the regulation in place.

Principle 76: Legal Accountability

Standard:

Countries should use existing laws and regulations or establish any such new laws or regulations to establish effective and proportionate administrative, civil, or criminal penalties for those who misuse charities for terrorist financing.[44]

Assessment:

From a legal perspective, Saudi Arabia is in partial compliance.

From an implementation/enforcement perspective, Saudi Arabia is not in compliance.

Law: Through SAMA, Saudi Arabia has established new regulations for those who misuse charities for terrorist financing. However, we have been unable to access these new regulations.

Enforcement / Implementation:

Further complicating efforts to regulate charitable contributions, members of the Saudi royal family have traditionally been immune to many of the laws and regulations issued by the Kingdom of Saudi Arabia. Lack of compliance among royal family members with regulations issued by the government form another obstacle to thorough and transparent regulatory regimes.

Some have accused the Saudi government itself of having donated to terrorist organizations. A document released to the press by the Israeli government and reportedly seized from Hamas offices in Gaza cites Hamas official Khaled Mashaal thanking the Saudi government for continuing "to send aid to the people through the civilian and popular channels, despite all the American pressures exerted on them." The official is reported to have sent the letter after meeting with Crown Prince Abdullah in October of 2002.[45] However, the AP report makes clear that "Saudi officials say their government's support for Palestinian causes, about US$80-million to US$100-million a year, goes solely to the Palestinian Authority, and that money raised among Saudis for Palestinians is intended for humanitarian purposes." Saudi foreign affairs advisor to Crown Prince Abdullah commented that the charge is "a ridiculous accusation," and that "no Saudi government money goes to Hamas, directly or indirectly."[46]

---

[44] Financial Action Task Force on Money Laundering, *Combating the abuse of Non-Profit Organizations International Best Practices*, October 11, 2002

[45] The New York Times, "Flow of Saudis' Cash to Hamas Scrutinized," September 17, 2003.

[46] The New York Times, "Flow of Saudis' Cash to Hamas Scrutinized," September 17, 2003.

Conclusions – Charities

Our review and analysis of Saudi Arabia's charities sector as regards ML/FT offenses has identified some areas in which that system is fully or substantially compliant with relevant international standards. However, there are also several issues of concern, which will require continuing attention:

1. Administration

The charities charter provides for transparency regarding the management of charitable institutions in Saudi Arabia. However, there is a major gap stemming from the traditional organization of charities and the lack of accountability.

2. Financial Transparency

The Saudi Arabian regulation of charitable financial transparency provides for financial accounting transparency, lacks rigor regarding the external auditing of charities' accounts and the interplay between charities and financial institutions.

3. *Programmatic Verification*

Saudi Arabian regulation does not provide a clear delineation of responsibilities regarding cooperation in the field of charities' oversight and solicitation of the identities of the donors and the beneficiaries of charitable donations. While it seems the cooperation between the U.S. and Saudi Arabia is mainly focused on law enforcement, preventive action against the misuse of charities has not taken place, to date, in the kingdom.

4. Oversight Bodies

In theory, there appear to be many government agencies in charge of regulating and supervising charities. However, the specific role of each of these agencies is unclear and this situation results in both gaps and overlap of authority. The method for supervising international branches of Saudi charities requires additional attention.

5. Sanctions

Legal accountability and potential sanctions are an area lacking clarity. This interferes with efforts to create a deterrent effect.

International Cooperation

This chapter will examine the international cooperation component of Saudi Arabia's AML/CTF effort along three themes:

1. Ratification of International Conventions
2. Internal Actions Taken by the Kingdom of Saudi Arabia
3. Conclusion

It is vital in the fight to impede terrorist financing that the international community secures a high level of international intelligence cooperation and information, especially from countries that are key transit and source points of terrorist funds. One of the most important findings of the various commissions and groups investigating the financing of the 9/11 hijackers is that although traditional AML provisions are effective for tracking the unusual transaction patterns associated with money laundering, they are not sufficient for tracking the smaller and less distinguishable transactions associated with terror financing. In fact, no single 'terrorist financial profile' would have enabled either domestic or foreign law enforcement agencies to detect and block the funds transmitted to the 9/11 hijackers. In interviews, both law enforcement experts and compliance officers emphasized that the best way to track terror financing is to share lists of suspected perpetrators and pay close attention to their accounts. This process requires streamlined information sharing and intelligence cooperation between and among governments and private sectors on an international basis. This makes intelligence cooperation and information sharing with the Saudi intelligence agencies, Saudi financial institutions, and Saudi enforcement authorities integral to effectively combating terrorist financing.

Ratification of International Conventions

International conventions on money laundering and terrorist financing are the basis of international cooperation. They outline a common definition of the problem at hand and a common approach to solving it. Should a country not accede to such a convention, there is a danger that it will fall out of step with the international community and create a gap in the international CTF regime.

Any analysis of Saudi Arabia's level of international cooperation must thus begin with an examination of the conventions to which they have acceded. The ratification of the treaty itself does not necessarily indicate that appropriate actions are being taken within the Kingdom to address the issue of terrorist financing. At a minimum, however, treaties act as benchmark for evaluating KSA's level of international cooperation.

It is important to examine two issues in attempting to evaluate Saudi Arabia's compliance with international treaties:

A. Is Saudi Arabia a signatory to the Vienna Convention, the Palermo Convention, and the United Nations International Convention for the Suppression of the Financing of Terrorism? Furthermore, is it a signatory to other important UN conventions pertaining to terrorism? If KSA is a signatory to these conventions, has it in fact ratified them?

   Though the Vienna Convention and the Palermo Convention do not specifically address terrorist financing, they do address issues related to money laundering. And though, as mentioned in the introduction to this chapter, a good AML regime is not necessarily a good CTF regime, AML efforts are foundational to monitoring the flow of suspicious funds.

B. Is Saudi Arabia implementing the international conventions cited above?

Principle 77: Compliance with International Money Laundering Treaties

Standard:

In accordance with FATF Recommendation 35[109], we have used the Vienna Convention and the Palermo Convention as the basis for assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal perspective Saudi Arabia is in substantial compliance with this principle. This principle is not applicable to enforcement.

Law:

Saudi Arabia signed the Palermo Convention in December 2000, and has not ratified it.[110] Saudi Arabia acceded to the Vienna Convention in January 1992.

We have thus not been able to verify Saudi Arabia's full compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's substantial compliance with the principle.

We have not seen any Saudi laws or regulations expressly implementing the terms of the Vienna Convention or the Palermo Convention. Articles 22-24 of the KSA-AMLL set forth guidelines for international cooperation.[111] Although these provisions are too vague to constitute effective implementation of the international cooperation components of the Vienna Convention or the Palermo Convention, they provide an encouraging legal basis for cooperation provisions in the forthcoming KSA-AMLL Implementation Rules.

Enforcement:

Enforcement issues are not applicable to this standard.

Implementation:

While it is not difficult to evaluate Saudi Arabia's compliance with the issue of signing an international convention, the second part of the standard, which addresses implementation, is broad and far-reaching. In order to effectively evaluate compliance with this standard it is necessary to examine the key components of the various treaties. Collectively, they address the following major elements relevant to terror financing:

1. The criminalization of money laundering
2. The empowerment of law enforcement authorities to freeze and confiscate assets associated with money laundering

---

[109] FATF35: Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

[110] Information on signature and ratification status is based on documents provided on the United Nations' website, at <http://untreaty.un.org/English/TreatyEvent2003/index.htm> (last visited on Nov. 13, 2003).

[111] Kingdom of Saudi Arabia, Regulations on Anti Money Laundering in KSA, Anti Money Laundering Law, August 2003, 6.

3. The obligation of regulatory authorities to establish a robust regulatory and supervisory regime for financial institutions
4. A smooth system of mutual legal assistance pertaining to AML and the encouragement of joint task forces and other methods of cooperation in addition to mutual legal assistance

A full evaluation of Saudi Arabia's compliance with these standards is outside the scope of this particular section, but is the subject of other parts of this report.

Principle 78: Ratification and Implementation of UN CFT Instruments

Standard:

In accordance with FATF Special Recommendation 1,[112] we have used the UN CFT Convention and the 2001 United Nations Security Council Resolution 1373 ("UNSC R1373") as the basis for assessing Saudi Arabia's compliance with this principle.

Assessment:

From a legal prospective Saudi Arabia is not in compliance with this principle. This principle is not applicable to enforcement.

Law:

Saudi Arabia signed the UN CFT Convention in November 2001, and has not ratified it.[113] UNSC R1373, adopted under Chapter VII of the UN Charter, is automatically mandatory on Saudi Arabia with no further action necessary on the kingdom's part. The offense of terrorist financing is set forth in the KSA-AMLL in Article 2(d).

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective. Our limited information tends to indicate that Saudi Arabia is non-compliant with the principle.

Saudi Arabia has failed to ratify the UN CFT Convention. We have not seen any laws or regulations expressly implementing the UN CFT Convention's terms, or the UNSC R1373. As described under Principle 42, the language in Article 2(d) of the KSA-AMLL cannot be considered as sufficiently implementing those two international documents.

Further, we note that Saudi Arabia is not a signatory to the 1997 International Convention for the Suppression of Terrorist Bombings (the "UN CTB Convention"), despite being called upon by the UNSC R1373 to "[b]ecome [a party] as soon as possible to the relevant international conventions and protocols relating to terrorism" (Article 3(d)).

Enforcement:

Enforcement issues are not applicable to this standard.

Implementation:

As discussed in Principle 35, the UN CTF is broad and far-reaching. The measures that Saudi Arabia has taken to implement some of the counter-terrorist financing measures described in it are discussed throughout this report.

---

[112] Each country should take immediate steps to ratify and to implement fully the 1999 United Nationas International Convention for the Suppression of the Financing of Terrorism. Countries should also immediately implement the United Nations resolutions relating to prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

[113] Information on signature and ratification status is based on documents provided on the United Nations' website, at <http://untreaty.un.org/ENGLISH/Status/Chapter_xviii/treaty11.asp> (last visited on Nov. 16, 2003).

Internal Actions Taken by KSA

As discussed in the introduction to this chapter, terrorist financing must be stopped through the exchange of information and assistance between and among governments and private institutions. That a country be a signatory of all the relevant conventions is important, but concrete measures must also be taken within its domestic regime. Most notably, Saudi Arabia's institutions must be authorized to share information with foreign authorities and empowered to take appropriate action to freeze and confiscate assets on the basis of international cooperation. Deficits in these areas could deny foreign authorities the information they need to track or prosecute terrorists or render fruitless foreign efforts to track finances to Saudi sources and transit points.

Principle 79: Authority for Prompt Response to Information-Sharing Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the legal authority for responding to information-sharing requests by foreign countries, we have looked at Article 7 of the Vienna Convention, Article 18 of the Palermo Convention, and Article 12 of the UN CFT Convention.[114]

Assessment:

We have been unable to verify Saudi Arabia's compliance with this principle from either a legal or an enforcement perspective.

Law:

The KSA-AMLL, in Article 22, provides authority for sharing information with law enforcement agencies of foreign countries.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's partial compliance with the principle.

Article 22 of the KSA-AMLL states that "Information disclosed by Financial and Non-Financial Institutions may be shared with concerned foreign authorities which are connected with the Kingdom through valid agreements or on the basis of reciprocity according to applicable legal procedures without prejudicing the confidentiality provisions and business practices of financial, non-financial and banking institutions."

Without access to the Implementation Rules, the vague terms of Article 22 make it difficult to verify its level of compliance with this principle. However, we note with concern several aspects of Article 22 that suggest that Saudi Arabia's compliance with this principle is partial at best:

a. *Requirement of Mutuality.*

The requirement in Article 22 of the KSA-AMLL that the concerned foreign authorities be "connected with the Kingdom through valid agreements or on the basis of reciprocity" appears to

---

[114] FATF 36: Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:
a. Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.
b. Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.
c. Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.
d. Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.
Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts .

contradict the language of relevant international documents. Article 7(7) of the Vienna Convention expressly contemplates mutual legal assistance, including the provision of information, to foreign countries that "are not bound by a treaty of mutual legal assistance." Article 7(15) of the same document lists permissible grounds for refusing mutual legal assistance; lack of a treaty or of reciprocity is not among them. Article 18(7) of the Palermo Convention, using similar language to Article 7(7) of the Vienna Convention, expressly provides for sharing of information with foreign countries that "are not bound by a treaty of mutual legal assistance." Article 18(21) of the Palermo Convention, corresponding to Article 7(15) of the Vienna Convention, lists permissible grounds for refusing a request for mutual legal assistance; again, lack of a treaty or of reciprocity is not among them. Furthermore, we are unaware of any bilateral, multilateral or regional agreements that 'connect' "foreign authorities" to Saudi Arabia and provide for mutual sharing of reported information.

It remains to be seen how the Implementation Rules will interpret the reciprocity requirement, and to what extent the requirement will inhibit, in violation of the Vienna and Palermo Conventions, the rendering of mutual legal assistance to foreign countries.

b. *Limited Scope.*

Article 22 of the KSA-AMLL grants authority to share information discovered by "Financial and Non-Financial Institutions." For a discussion of the limited scope of this term, and in particular its exclusion of the non-profit sector, see Principle 2b.

c. *Limited Range of Assistance.*

The KSA-AMLL grants authority to share "information" that has been "discovered." It is unclear, pending publication of the Implementation Rules, whether this covers the provision of evidentiary items, expert evaluations, originals or certified copies of relevant documents and records, "including government, bank, financial, corporate or business records," as contemplated by Article 18(3)(e)-(f) of the Palermo Convention. (Corresponding language appears in Article 7(2)(e)-(f) of the Vienna Convention.)

d. *Role of Bank Secrecy.*

The degree of international cooperation that the AMLL allows is further circumscribed by bank secrecy stipulations. Article 22, as quoted above, indicates that banks may not violate confidentiality provisions in cooperating with foreign authorities. Although we have not seen the Saudi bank secrecy regulations, we have no reason to believe that they make allowances for sharing confidential information with foreign authorities. The "confidentiality provisions" override is the most serious obstacle to compliance with this standard. It is noteworthy in this regard that the United Nations Convention against Transnational Organized Crime (the "Palermo Convention"), of which Saudi Arabia is a signatory and which is used by FATF as a benchmark for assessing AML compliance, declares that "States Parties shall not decline to render mutual legal assistance pursuant to this article on the ground of bank secrecy" (Article 18(8)).

e. *Legal Procedure*

We are unaware of any "applicable legal procedure" for effecting such information exchange. Perhaps this will be addressed in the Implementation Laws.

f. *Designated Authority*

The Palermo Convention requires States Parties to "designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution" (Article 8(13)). The KSA-AMLL does not designate a Saudi authority to which foreign authorities should address their requests for information. SAMA Regulations indicate that banks should cooperate with international parties through SAMA, but it is not clear that SAMA is the point of contact for foreign governments.[115]

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

Because intelligence collaboration and information sharing between governments and between financial bodies tends to be kept confidential, measuring Saudi implementation in this regard is extremely difficult. Our limited findings indicate that Saudi Arabia has taken steps since September 11, 2001 and the Riyadh bombings in May 2003 to cooperate more effectively with international enforcement agencies. One important sign of increased international cooperation has been the implementation of a Joint U.S.-Saudi Task Force devoted to the issue of terrorist financing. The joint task force was reportedly agreed to after a July 2003 phone call between President Bush and Saudi Crown Prince Abdullah.[116] Apparently, the task force agreement was finalized during a visit of senior NSC, State, and Treasury officials to Saudi Arabia in August.[117] This United States-Saudi CTF relationship has led to at least two specific cooperative initiatives. According to John Pistole, Assistant Director, counter-terrorism division, FBI, there has been significant cooperation between FBI and *the Mabahith* (Saudi Arabia's internal intelligence agency).[118] He testified that joint FBI-Mabahith operations are on-going. In addition, Saudi Arabia has established the joint task force with the FBI and IRS in Saudi Arabia since the May 12 2003 bombings in Saudi Arabia.[119] Detailed information on these activities is unavailable and at this point it is too early to assess the joint task force's work. Still, the existence of the task force and the FBI and IRS programs implies that some sort of understanding for information sharing exists between the United States and Saudi Arabia.

Too much should not be assumed about U.S.-Saudi cooperation, however. Matthew Levitt, a senior fellow at The Washington Institute for Near East Policy and a former FBI analyst specializing in terror financing, says that the joint task force is still experiencing problems in terms of cooperation.[120] Instead of being given access to a wide variety of sources and data, FBI agents must

[115] SAMA AML-CTF Article 5.3
[116] Farah, Douglas. *Washington Post*, http://stacks.msnbc.com/news/957318.asp (last visited on November 15, 2003).
[117] Farah, Douglas. *Washington Post*, http://stacks.msnbc.com/news/957318.asp (last visited on November 15, 2003).
[118] Pistole, John, testimony before the House committee on financial services, Sept. 24, 2003.
[119] FBI Director Rober Mueller, June 2, 2003, "After the May 12 incidents in Riyadh, the US sent experts to the Kingdom for technical assistance."
[120] Levitt, Matthew, Washington Institute for Near East Policy, interview, 11/12/03.

make very specific requests for information in order to obtain it.[121] Unfortunately, successful law enforcement operations of this sort require access to a great deal of information; based on what investigators see, they can then pursue the proper specific details. Levitt believes that American law enforcement agents are not getting this necessary initial access.

We have two further reasons to be concerned that adequate information-sharing measures are not being implemented. First, Section 5.3 of SAMA's Rules Governing Anti Money Laundering and Combating Terrorist Financing states that banks must conduct all of their international cooperation and information sharing through SAMA.[122] This eliminates communication and cooperation between financial institutions on a transnational level. Interviews with former senior bankers at Saudi banks indicate that joint venture banks, which are partially owned by foreign firms, are not allowed to communicate information relevant to ML and TF to their parent companies without first going through SAMA.[123]

Secondly, barriers to information-sharing likely extend beyond confidentiality regulations and other legal short-comings. The ingrained practice of not engaging in such sharing, which was attested to by senior banking executives with whom we spoke, might well prove resilient to legislation and enforcement, and create an independent obstacle to implementing effective international cooperation.[124]

This study cannot definitively judge whether or not Saudi Arabia is cooperating on a satisfactory level with foreign authorities. This is due primarily to the fact that much of the information is classified and many members in the American government do not wish to speak about such a controversial issue. However, the information available indicates that while Saudi Arabia has made strides in increasing international cooperation, there is still much room for improvement.

[121] Levitt, Matthew, Washington Institute for Near East Policy, interview, 11/12/03.
[122] Rules Governing Anti Money Laundering and Combating Terrorist Financing, 12.
[123] Interview with former senior SAMBA employee, November 12 2003, and Interview with compliance officer at large international bank October 7, 2003.
[124] Interview with former senior SAMBA employee, November 12 2003, and Interview with compliance officer at large international bank October 7, 2003.

Principle 80: Authority for Prompt Response to Investigation-Assistance Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the legal authority for responding to investigation-assistance requests by foreign countries, we have looked at Article 7 of the Vienna Convention, Article 18 of the Palermo Convention, and Article 12 of the UN CFT Convention.

Assessment:

From both a legal and enforcement perspective we have been unable to verify Saudi Arabia's compliance with this principle.

Law:

The KSA-AMLL, in Article 23, provides authority for assisting investigations of law enforcement agencies of foreign countries.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's partial compliance with the principle.

Article 23 of the KSA-AMLL states that Saudi authorities, "upon a request from a concerned authority in a foreign country connected with the kingdom through ratified agreements or on the basis of reciprocity may order the pursuing of property, proceeds and instrumentalities connected with money laundering in accordance with Saudi applicable regulations."

Without access to the Implementation Rules, the vague terms of Article 23 make it difficult to verify its level of compliance with this principle. Our concerns with Article 23 echo those we have with Article 22 in Principle 36a; several aspects of Article 23 that suggest that Saudi Arabia's compliance with Principle 36b is partial at best:

a. *Requirement of Mutuality.*

See corresponding section in Principle 36a for discussion.

b. *Limited Range of Assistance.*

The KSA-AMLL grants authority to "pursue" assets on behalf of foreign authorities. It is unclear, pending publication of the Implementation Rules, whether this authority extends to taking evidence or statements from persons, effecting service of judicial documents, executing searches and seizures, examining objects and sites, and facilitating the voluntary appearance of persons in the requesting State Party, as contemplated by Article 18(3) of the Palermo Convention. (Corresponding language appears in Article 7(2) of the Vienna Convention.)

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

See corresponding section in Principle 36a for discussion

Principle 81: Authority for Prompt Response to Asset-Freezing Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the legal authority for responding to asset-freezing requests by foreign countries, we have looked at Articles 5 and 7 of the Vienna Convention, Articles 12, 13 and 18 of the Palermo Convention, and Article 12 of the UN CFT Convention.[125]

Assessment:

We have not been able to verify Saudi Arabia's compliance with this principle from either a legal or an enforcement perspective.

Law:

The KSA-AMLL, in Article 23, provides authority for freezing assets based on requests by law enforcement agencies of foreign countries.

We have not been able to verify Saudi Arabia's compliance with this principle from a legal perspective. Our limited information tends to indicate Saudi Arabia's partial compliance with the principle.

Article 23 of the KSA-AMLL states that Saudi courts may, "pursuant to a request by a court or concerned authority in a foreign country connected with the kingdom through ratified agreements or on the basis of reciprocity, order the impounding of property, proceeds or instrumentalities connected with money laundering in accordance with Saudi applicable regulations."

Our concerns with Article 23 in regard to this principle are similar to those concerns discussed in Principle 36a and 36b. Without access to the Implementation Rules, the vague terms of Article 23 make it difficult to verify its level of compliance with this principle. Several aspects of Article 23 that suggest that Saudi Arabia's compliance with Principle 38a is partial at best:

a. *Requirement of Mutuality.*

See corresponding section in Principle 36a for discussion.

b. *Limited Range of Assistance.*

The KSA-AMLL grants authority to "impound" assets pursuant to requests by foreign authorities. It is unclear, pending publication of the Implementation Rules, whether this authority covers taking "measures to identify, trace and freeze or seize" the assets as contemplated by Article

[125] FATF38: There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.

13(2) of the Palermo Convention. (Corresponding language appears in Article 5(4)(b) of the Vienna Convention.)

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

Very little information is available in this regard. A document released by the Saudi embassy in Washington states that "Saudi Arabia on September 26, 2001 required Saudi banks to identify and freeze all assets relating to terrorist suspects and entities per the list issued by the US government on September 23, 2001," it is unknown whether this action was taken or how many assets were frozen.[126] Saudi Arabia has claimed to seize terrorist assets but it is unknown whether these seizures were the resulted of coordination with other countries.

The government of Saudi Arabia has also released information on two related cases. In March of 2002, Saudi and the United States jointly blocked the accounts of the Bosnia and Somalia branches of Al-Haramain Islamic Foundation. In September 2002, US Treasury and Saudi government took joint action, freezing the assets of the Rabita Trust, and those of its director Wa'el Hamza Julaidan, an associate of Osama bin Laden.[127] It is known that both these cases were based on US information and requests for enforcement.

In addition, Saudi Arabia has stated that a special committee was established, drawing from the Ministry of Interior, Ministry of Foreign Affairs, the Intelligence Agency and SAMA, to deal with requests from international bodies and countries with regard to combating terrorist financing.[128] However, there is no information available on this committee.

In regard to implementation, we would like information on the following questions:

1) With which governments does Saudi Arabia have a reciprocal agreement to cooperate on AML-CTF matters?
2) How many requests have foreign governments submitted to Saudi Arabia for action on specific CTF cases?
3) How has Saudi Arabia responded to these requests?
4) What is the process by which assets are seized in Saudi Arabia?
5) What happens to assets seized in Saudi Arabia as the result of an international investigation?

[126] A document released by Saudi Embassy in the US, "Initiatives and Actions Taken by the KSA in the Financial Area to Combat Terrorism," p. 6.
[127] A document released by Saudi Embassy in the US, "Initiatives and Actions Taken by the KSA in the Financial Area to Combat Terrorism," p.2
[128] A document released by Saudi Embassy in the US, "Initiatives and Actions Taken by the KSA in the Financial Area to Combat Terrorism," p.2

Principle 82: Authority for Prompt Response to Confiscation Judgment-Executing Requests by Foreign Countries

Standard:

We have used the Vienna Convention, the Palermo Convention, and the UN CFT Convention for guidance in assessing Saudi Arabia's compliance with this principle. Specifically, in assessing the legal authority for responding to confiscation requests by foreign countries, we have looked at Article 5 of the Vienna Convention, and Articles 12 and 13 of the Palermo Convention.

Assessment:

From a legal perspective we have found Saudi Arabia to be partially compliant with this principle. From an enforcement perspective we have been unable to determine Saudi Arabia's compliance.

Law:

The KSA-AMLL, in Article 24, provides authority for confiscating assets based on rulings by courts of foreign countries.

We have found Saudi Arabia to be partially compliant with this principle from a legal perspective.

Article 24 of the KSA-AMLL states that rulings by foreign courts "providing for the confiscation of property, proceeds or instrumentalities connected with money laundering, issued by a competent court in a foreign country connected with the kingdom through a valid agreement or convention, or on the basis of reciprocity, may be recognized by the kingdom if the property, proceeds or instrumentalities covered by the court ruling are subject to confiscation under Saudi applicable law."

We do not consider the Article 24 language to be only partially with this principle for the following reasons:

a. *Requirement of Mutuality.*

The requirement in Article 24 of the KSA-AMLL that the concerned foreign authorities be "connected with the Kingdom through a valid agreement or convention, or on the basis of reciprocity" appears to contradict the language of relevant international documents. Article 5(4)(a) of the Vienna Convention requires a Party in whose territory confiscable assets are situated, upon receiving a request from "another Party having jurisdiction over [a relevant] offence," to submit the requesting Party's order of confiscation to the requested Party's "competent authorities, with a view to giving it effect to the extent requested." No limits are imposed on the requesting Party's identity other than its having jurisdiction over the relevant offense. The Palermo Convention contains corresponding language in its Article 13(1).

By imposing a requirement that the requesting Party be connected to the Kingdom, Article 24 of the KSA-AMLL appears to constrain its grant of authority to respond to asset-confiscation rulings by foreign courts, in a manner inconsistent with international documents.

b. *Hortatory Language.*

The KSA-AMLL indicates that rulings by foreign courts "may" be recognized by the kingdom. This contrasts unfavorably with the language of the Vienna Convention, which provides in Article 5(4)(a) that a requested Party "shall" submit the order of confiscation to its competent authorities with a view to giving effect to it. The Palermo Convention contains corresponding language in its Article 13(1).

c. *Limits of Saudi confiscatory powers.*

The language in Article 24 of the KSA-AMLL conditions the confiscation of assets upon such assets' being subject to confiscation under Saudi applicable law. For a discussion of the limits of Saudi applicable law, see Principle 3.

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

See corresponding section in Principle 38a for discussion

Principle 83: Extradition for ML and FT

Standard:

We have used FATF recommendation 39[129] in assessing Saudi Arabia's compliance with this principle.

Assessment

From a legal perspective we have found that Saudi Arabia we are not able to verify Saudi Arabia's compliance with this principle. From enforcement perspective we are not be able to verify Saudi Arabia's compliance with the principle.

Law:

There are no laws and procedures that specifically address the extradition of individuals charged with a ML or FT.

AML Articles 22-24, on the basis of reciprocity, deal broadly with international cooperation. However, they address information sharing and asset tracking and seizure only; no mention is made of the fate of the perpetrators.

While it would to desirable to see specific mention of extradition made in Saudi AML-CTF laws, it must be noted that Saudi Arabia is not bound to extradite for offense that it undertakes to prosecute itself. See the Criminal Law chapter for an analysis of Saudi Arabia's ability to try individuals for FT.

Enforcement:

We are unaware of any enforcement measures taken by Saudi Arabia in regard to this principle.

Implementation:

We are not aware of any efforts on the part of a foreign government to extradite an individual charged with ML or FT from Saudi Arabia.

---

[129] Countries should recognize money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings

Conclusions – International Cooperation

In evaluating Saudi Arabia's level of international cooperation we have found the following outstanding issues.

1. Ratification of Treaties

Saudi Arabia has yet to ratify the Palermo Convention on international crime or the UN CFT Convention. These two documents embody the international consensus on combating money laundering and terrorist financing. The fact that Saudi Arabia has not ratified them raises the concern that the Kingdom does not see the challenge at hand or its solution in the same way as much of the rest of the international community. A disagreement on either of these points is likely to hinder the necessary cooperative effort.

It is also of concern that Saudi Arabia has neither signed nor ratified the 1997 UN Convention on Terror Bombing. Any disagreement on what constitutes an act of terrorism could impede international efforts to gain Saudi cooperation to track and prosecute individuals that the Kingdom does not consider terrorists.

2. Vagueness of the Laws

Article 22-24 of the new AML laws outline requirements pertaining to international cooperation. However, these laws are vague, and we hope that additional requirements will be included in the new implementation laws pertaining to the AML law.

3. Role of Banking Secrecy

Saudi Arabia has several laws that could impede international cooperation, most particularly Article 22 of the KSA-AMLL. Although we have not seen the Saudi bank secrecy regulations, we have no reason to believe that they make allowances for sharing confidential information with foreign authorities.

4. Law Enforcement Cooperation

We have very little information on Saudi cooperation with foreign law enforcement agencies, but there is some indication that U.S. authorities are not getting the cooperation they need from their Saudi counterparts.

Annex 1

The Forty Recommendations (2003)

LEGAL SYSTEMS

Scope of the criminal offence of money laundering

Recommendation 1

Countries should criminalise money laundering on the basis of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) and the 2000 United Nations Convention on Transnational Organized Crime (the Palermo Convention).

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences which are punishable by a maximum penalty of more than one year's imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences [3].

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

Footnotes:

[3] See the definition of "designated categories of offences" in the Glossary.

Recommendation 2

Countries should ensure that:

a. The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

b. Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.

Provisional measures and confiscation

Recommendation 3

Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property which is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.

MEASURES TO BE TAKEN BY FINANCIAL INSTITUTIONS AND NON-FINANCIAL BUSINESSES AND PROFESSIONS TO PREVENT MONEY LAUNDERING AND TERRORIST FINANCING

Recommendation 4

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.

Customer due diligence and record-keeping

Recommendation 5

Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information [4] .

b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c. Obtaining information on the purpose and intended nature of the business relationship.

d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.
(See Interpretative Notes: Recommendation 5 and Recommendations 5, 12 and 16) /

Footnotes:

[4] Reliable, independent source documents, data or information will hereafter be referred to as "identification data".

Recommendation 6

Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a. Have appropriate risk management systems to determine whether the customer is a politically exposed person.

b. Obtain senior management approval for establishing business relationships with such customers.

c. Take reasonable measures to establish the source of wealth and source of funds.

d. Conduct enhanced ongoing monitoring of the business relationship.

(See Interpretative Note)

Recommendation 7

Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a. Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

b. Assess the respondent institution's anti-money laundering and terrorist financing controls.

c. Obtain approval from senior management before establishing new correspondent relationships.

d. Document the respective responsibilities of each institution.

e. With respect to "payable-through accounts", be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts

of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

Recommendation 8

Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions.

Recommendation 9

Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a) – (c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a. A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a) – (c) of the CDD process. Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

b. The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations. ***(See Interpretative Note)***

Recommendation 10

Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority. ***(See Interpretative Note)***

Recommendation 11

Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors. ***(See Interpretative Note)***

Recommendation 12

The customer due diligence and record-keeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:

a. Casinos – when customers engage in financial transactions equal to or above the applicable designated threshold.

b. Real estate agents - when they are involved in transactions for their client concerning the buying and selling of real estate.

c. Dealers in precious metals and dealers in precious stones - when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

d. Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:

- buying and selling of real estate;
- managing of client money, securities or other assets;
- management of bank, savings or securities accounts;
- organisation of contributions for the creation, operation or management of companies;
- creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e. Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

(See Interpretative Note)

Reporting of suspicious transactions and compliance

Recommendation 13

If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU). ***(See Interpretative Note)***

Recommendation 14

Financial institutions, their directors, officers and employees should be:

a. Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b. Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

(See Interpretative Note)

Recommendation 15

Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a. The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

b. An ongoing employee training programme.

c. An audit function to test the system.

(See Interpretative Note)

Recommendation 16

The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a. Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b. Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c. Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege. ***(See Interpretative Notes: Recommendation 16 and Recommendations 5, 12, and 16)***

Other measures to deter money laundering and terrorist financing

Recommendation 17

Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

Recommendation 18

Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

Recommendation 19

Countries should consider:

a. Implementing feasible measures to detect or monitor the physical cross-border transportation of currency and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

b. The feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

Recommendation 20

Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

Recommendation 21

Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

Recommendation 22

Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

Regulation and supervision

Recommendation 23

Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing. ***(See Interpretative Note)***

Recommendation 24

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a. Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist-financing measures. At a minimum:

    - casinos should be licensed;
    - competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino

- competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

b. Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.

Recommendation 25

The competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions. ***(See Interpretative Note)***

INSTITUTIONAL AND OTHER MEASURES NECESSARY IN SYSTEMS FOR COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

Competent authorities, their powers and resources

Recommendation 26

Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR. ***(See Interpretative Note)***

Recommendation 27

Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries. ***(See Interpretative Note)***

Recommendation 28

When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

Recommendation 29

Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

Recommendation 30

Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.

Recommendation 31

Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

Recommendation 32

Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

Transparency of legal persons and arrangements

Recommendation 33

Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

Recommendation 34

Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settlor, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.

INTERNATIONAL CO-OPERATION

Recommendation 35

Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Mutual legal assistance and extradition

Recommendation 36

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

a. Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance.

a. Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b. Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c. Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection. ***(See Interpretative Note)***

GLOSSARY

In these Recommendations the following abbreviations and references are used:

"**Beneficial owner**" refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

"**Core Principles**" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

"**Designated categories of offences**" means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;

b. Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests.

c. Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters.

d. Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.

Recommendation 37

Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.

Recommendation 38

There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets. ***(See Interpretative Note)***

Recommendation 39

Countries should recognise money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should take their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgements, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

Other forms of co-operation

Recommendation 40

Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and
- insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

"**Designated non-financial businesses and professions**" means:

a. Casinos (which also includes internet casinos).

b. Real estate agents.

c. Dealers in precious metals.

d. Dealers in precious stones.

e. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f. Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
- acting as (or arranging for another person to act as) a trustee of an express trust;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

"**Designated threshold**" refers to the amount set out in the Interpretative Notes.

"**Financial institutions**" means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[5]
2. Lending.[6]
3. Financial leasing.[7]
4. The transfer of money or value.[8]

5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).

6. Financial guarantees and commitments.

7. Trading in:

    a. money market instruments (cheques, bills, CDs, derivatives etc.);

    b. foreign exchange;

    c. exchange, interest rate and index instruments;

    d. transferable securities;

    e. commodity futures trading.

8. Participation in securities issues and the provision of financial services related to such issues.

9. Individual and collective portfolio management.

10. Safekeeping and administration of cash or liquid securities on behalf of other persons.

11. Otherwise investing, administering or managing funds or money on behalf of other persons.

12. Underwriting and placement of life insurance and other investment related insurance.[9]

13. Money and currency changing.

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

Footnotes:

[5] This also captures private banking.
[6] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).
[7] This does not extend to financial leasing arrangements in relation to consumer products.
[8] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.
[9] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

"**FIU**" means financial intelligence unit.

"**Legal arrangements**" refers to express trusts or other similar legal arrangements.

"**Legal persons**" refers to bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.

"**Payable-through accounts**" refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

"**Politically Exposed Persons**" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories.

"**Shell bank**" means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.

"**STR**" refers to suspicious transaction reports.

"**Supervisors**" refers to the designated competent authorities responsible for ensuring compliance by financial institutions with requirements to combat money laundering and terrorist financing.

"**the FATF Recommendations**" refers to these Recommendations and to the FATF Special Recommendations on Terrorist Financing.

Annex 2

FATF Special Recommendations on Terrorist Financing

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts. For further information on the Special Recommendations as related to the self-assessment process, see the Guidance Notes.

I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations. **(See Interpretative Note) (See Best Practices Paper)**

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

VI. Alternative remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions. **(See Interpretative Note) (See Best Practices Paper)**

VII. Wire transfers

Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain.

Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number). **(See Interpretative Note)**

VIII. Non-profit organisations

Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

i. by terrorist organisations posing as legitimate entities;

ii. to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

iii. to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.

Annex 3

Basel Committee on Banking Supervision

Customer due diligence for banks
October 2001

Working Group on Cross-border Banking

Co-Chairs:

Mr Charles Freeland, Deputy Secretary General, Basel Committee on Banking Supervision

Mr Colin Powell, Chairman, Offshore Group of Banking Supervisors, and Chairman, Jersey Financial Services Commission

Bermuda Monetary Authority Mr D Munro Sutherland

Cayman Islands Monetary Authority Mr John Bourbon
Mrs Anna McLean

Banque de France/Commission Bancaire Mr Laurent Ettori

Federal Banking Supervisory Office of Germany Mr Jochen Sanio
Mr Peter Kruschel

Guernsey Financial Services Commission Mr Peter G Crook (until April 2001)
Mr Philip Marr (since April 2001)

Banca d'Italia Mr Giuseppe Godano

Financial Services Agency, Japan Mr Kiyotaka Sasaki (until July 2001)
Mr Hisashi Ono (since July 2001)

Commission de Surveillance du Secteur Financier,
Luxembourg
Mr Romain Strock

Monetary Authority of Singapore Mrs Foo-Yap Siew Hong
Ms Teo Lay Har

Swiss Federal Banking Commission Mr Daniel Zuberbühler
Ms Dina Balleyguier

Financial Services Authority, United Kingdom Mr Richard Chalmers

Board of Governors of the Federal Reserve System Mr William Ryback

Federal Reserve Bank of New York Ms Nancy Bercovici

Office of the Comptroller of the Currency Mr Jose Tuya
Ms Tanya Smith

Secretariat Mr Andrew Khoo

Table of Contents

Customer due diligence for banks

I. Introduction

1. Supervisors around the world are increasingly recognising the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

2. In reviewing the findings of an internal survey of cross-border banking in 1999, the Basel Committee identified deficiencies in a large number of countries' know-your-customer (KYC) policies for banks. Judged from a supervisory perspective, KYC policies in some countries have significant gaps and in others they are non-existent. Even among countries with well-developed financial markets, the extent of KYC robustness varies. Consequently, the Basel Committee asked the Working Group on Cross-border Banking[130] to examine the KYC procedures currently in place and to draw up recommended standards applicable to banks in all countries. The resulting paper was issued as a consultative document in January 2001. Following a review of the comments received, the Working Group has revised the paper and the Basel Committee is now distributing it worldwide in the expectation that the KYC framework presented here will become the benchmark for supervisors to establish national practices and for banks to design their own programmes. It is important to acknowledge that supervisory practices of some jurisdictions already meet or exceed the objective of this paper and, as a result, they may not need to implement any changes.

3. KYC is most closely associated with the fight against money-laundering, which is essentially the province of the Financial Action Task Force (FATF).[131] It is not the Committee's intention to duplicate the efforts of the FATF. Instead, the Committee's interest is from a wider prudential perspective. Sound KYC policies and procedures are critical in protecting the safety and soundness of banks and the integrity of banking systems. The Basel Committee and the Offshore Group of Banking Supervisors (OGBS) continue to support strongly the adoption and implementation of the FATF recommendations, particularly those relating to banks, and intend the standards in this paper to be consistent with the FATF recommendations. The Committee and the OGBS will also consider the adoption of any higher standards introduced by the FATF as a result of its current review of the 40 Recommendations. Consequently, the Working Group has been and will remain in close contact with the FATF as it develops its thoughts.

4. The Basel Committee's approach to KYC is from a wider prudential, not just anti money laundering, perspective. Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities.

5. The Basel Committee's interest in sound KYC standards originates from its concerns for market integrity and has been heightened by the direct and indirect losses incurred by banks due to their

[130] This is a joint group consisting of members of the Basel Committee and of the Offshore Group of Banking Supervisors.

[131] The FATF is an inter-governmental body which develops and promotes policies, both nationally and internationally, to combat money laundering. It has 29 member countries and two regional organisations. It works in close cooperation with other international bodies involved in this area such as the United Nations, Office for Drug Control and Crime Prevention, the Council of Europe, the Asia-Pacific Group on Money Laundering and the Caribbean Financial Action Task Force. The FATF defines money laundering as the processing of criminal proceeds in order to disguise their illegal origin.

lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the banks' reputation significantly diminished had the banks maintained effective KYC programmes.

6. This paper reinforces the principles established in earlier Committee papers by providing more precise guidance on the essential elements of KYC standards and their implementation. In developing this guidance, the Working Group has drawn on practices in member countries and taken into account evolving supervisory developments. The essential elements presented in this paper are guidance as to minimum standards for worldwide implementation for all banks. These standards may need to be supplemented and/or strengthened, by additional measures tailored to the risks of particular institutions and risks in the banking system of individual countries. For example, enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers. In a number of specific sections in this paper, there are recommendations for higher standards of due diligence for higher risk areas within a bank, where applicable.

7. The need for rigorous customer due diligence standards is not restricted to banks. The Basel Committee believes similar guidance needs to be developed for all non-bank financial institutions and professional intermediaries of financial services such as lawyers and accountants.

II. Importance of KYC standards for supervisors and banks

8. The FATF and other international groupings have worked intensively on KYC issues, and the FATF's 40 Recommendations on combating money-laundering[132] have international recognition and application. It is not the intention of this paper to duplicate that work.

9. At the same time, sound KYC procedures have particular relevance to the safety and soundness of banks, in that:

- they help to protect banks' reputation and the integrity of banking systems by reducing the likelihood of banks becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;

- they constitute an essential part of sound risk management (e.g. by providing thebasis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

10. The inadequacy or absence of KYC standards can subject banks to serious customer and counterparty risks, especially ***reputational, operational, legal and concentration risks***. It is worth noting that all these risks are interrelated. However, any one of them can result in significant financial cost to banks (e.g. through the withdrawal of funds by depositors, the termination of inter-bank facilities, claims against the bank, investigation costs, asset seizures and freezes, and loan losses), as well as the need to divert considerable management time and energy to resolving problems that arise.

11. ***Reputational risk*** poses a major threat to banks, since the nature of their business requires maintaining the confidence of depositors, creditors and the general marketplace. Reputational risk is defined as the potential that adverse publicity regarding a bank's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution. Banks are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect

[132] See FATF recommendations 10 to 19 which are reproduced in Annex 2

themselves by means of continuous vigilance through an effective KYC programme. Assets under management, or held on a fiduciary basis, can pose particular reputational dangers.

12. ***Operational risk*** can be defined as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the KYC context relates to weaknesses in the implementation of banks' programmes, ineffective control procedures and failure to practise due diligence. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the bank.

13. ***Legal risk*** is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of a bank. Banks may become subject to lawsuits resulting from the failure to observe mandatory KYC standards or from the failure to practise due diligence. Consequently, banks can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors. Indeed, a court case involving a bank may have far greater cost implications for its business than just the legal costs. Banks will be unable to protect themselves effectively from such legal risks if they do not engage in due diligence in identifying their customers and understanding their business.

14. Supervisory concern about ***concentration risk*** mostly applies on the assets side of the balance sheet. As a common practice, supervisors not only require banks to have information systems to identify credit concentrations but most also set prudential limits to restrict banks' exposures to single borrowers or groups of related borrowers. Without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for a bank to measure its concentration risk. This is particularly relevant in the context of related counterparties and connected lending.

15. On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the bank's liquidity. Funding risk is more likely to be higher in the case of small banks and those that are less active in the wholesale markets than large banks. Analysing deposit concentrations requires banks to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors. It is essential that liabilities managers in small banks not only know but maintain a close relationship with large depositors, or they will run the risk of losing their funds at critical times.

16. Customers frequently have multiple accounts with the same bank, but in offices located in different countries. To effectively manage the reputational, compliance and legal risk arising from such accounts, banks should be able to aggregate and monitor significant balances and activity in these accounts on a fully consolidated worldwide basis, regardless of whether the accounts are held on balance sheet, off balance sheet, as assets under management, or on a fiduciary basis.

17. Both the Basel Committee and the Offshore Group of Banking Supervisors are fully convinced that effective KYC practices should be part of the risk management and internal control systems in all banks worldwide. National supervisors are responsible for ensuring that banks have minimum standards and internal controls that allow them to adequately know their customers. Voluntary codes of conduct[133] issued by industry organisations or associations can be of considerable value in underpinning regulatory guidance, by giving practical advice to banks on operational matters. However, such codes cannot be regarded as a substitute for formal regulatory guidance.

III. Essential elements of KYC standards

[133] An example of an industry code is the "Global anti-money-laundering guidelines for Private Banking" (also called the Wolfsberg Principles) that was drawn up in October 2000 by twelve major banks with significant involvement in private banking.

18. The Basel Committee's guidance on KYC has been contained in the following three papers and they reflect the evolution of the supervisory thinking over time. *The Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* issued in 1988 stipulates the basic ethical principles and encourages banks to put in place effective procedures to identify customers, decline suspicious transactions and cooperate with law enforcement agencies. The 1997 *Core Principles for Effective Banking Supervision* states, in a broader discussion of internal controls, that banks should have adequate policies, practices and procedures in place, including strict "know-your-customer" rules; specifically, supervisors should encourage the adoption of the relevant recommendations of the FATF. These relate to customer identification and record-keeping, increased diligence by financial institutions in detecting and reporting suspicious transactions, and measures to deal with countries with inadequate anti-money laundering measures. The 1999 *Core Principles Methodology* further elaborates the Core Principles by listing a number of essential and additional criteria. (Annex 1 sets out the relevant extracts from the *Core Principles* and the *Methodology*.)

19. All banks should be required to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements"[134]. Certain key elements should be included by banks in the design of KYC programmes. Such essential elements should start from the banks' risk management and control procedures and should include (1) customer acceptance policy, (2) customer identification, (3) on-going monitoring of high risk accounts and (4) risk management. Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC should be a core feature of banks' risk management and control procedures, and be complemented by regular compliance reviews and internal audit. The intensity of KYC programmes beyond these essential elements should be tailored to the degree of risk.

1. Customer acceptance policy

20. Banks should develop clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk to a bank. In preparing such policies, factors such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered. Banks should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with higher risk customers, such as politically exposed persons (see section 2.2.3 below), should be taken exclusively at senior management level.

2. Customer identification

21. Customer identification is an essential element of KYC standards. For the purposes of this paper, a customer includes:

- the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners);

[134] *Core Principles Methodology*, Essential Criterion 1

- the beneficiaries of transactions conducted by professional intermediaries; and
- any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the bank.

22. Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.

23. Banks should "document and enforce policies for identification of customers and those acting on their behalf".[135] The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. Special attention should be exercised in the case of non-resident customers and in no case should a bank short-circuit identity procedures just because the new customer is unable to present himself for interview. The bank should always ask itself why the customer has chosen to open an account in a foreign jurisdiction.

24. The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, there is a need for banks to undertake regular reviews of existing records[136]. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated.
However, if a bank becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

25. Banks that offer private banking services are particularly exposed to reputational risk, and should therefore apply enhanced due diligence to such operations. Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the bank does not diligently follow established KYC procedures. All new clients and new accounts should be approved by at least one person, of appropriate seniority, other than the private banking relationship manager. If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

26. Banks should develop "clear standards on what records must be kept on customer identification and individual transactions and their retention period"[137]. Such a practice is essential to permit a bank to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution. As the starting point and natural follow-up of the identification process, banks should obtain customer identification papers and retain copies of them for at least five years after an account is closed. They should also retain all financial transaction records for at least five years after the transaction has taken place.

2.1 General identification requirements

27. Banks need to obtain all information necessary to establish to their full satisfaction the identity of each new customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal, corporate, etc.) and the expected size of the account. National supervisors are encouraged to provide guidance to assist

[135] *Core Principles Methodology*, Essential Criterion 2.
[136] The application of new KYC standards to existing accounts is currently subject to FATF review.
[137] *Core Principles Methodology*, Essential Criterion 2.

banks in designing their own identification procedures. The Working Group intends to develop essential elements of customer identification requirements.

28. When an account has been opened, but problems of verification arise in the banking relationship which cannot be resolved, the bank should close the account and return the monies to the source from which they were received[138]

29. While the transfer of an opening balance from an account in the customer's name in another bank subject to the same KYC standard may provide some comfort, banks should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one bank to another. However, if a bank has any reason to believe that an applicant is being refused banking facilities by another bank, it should apply enhanced diligence procedures to the customer.

30. Banks should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered[139] accounts function as anonymous accounts but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the account-holder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a bank's compliance function or from the supervisors.

2.2 Specific identification issues

31. There are a number of more detailed issues relating to customer identification which need to be addressed. Several of these are currently under consideration by the FATF as part of a general review of its 40 recommendations, and the Working Group recognises the need to be consistent with the FATF.

2.2.1 Trust, nominee and fiduciary accounts

32. Trust, nominee and fiduciary accounts can be used to circumvent customer identification procedures. While it may be legitimate under certain circumstances to provide an extra layer of security to protect the confidentiality of legitimate private banking customers, it is essential that the true relationship is understood. Banks should establish whether the customer is taking the name of another customer, acting as a "front", or acting on behalf of another person as trustee, nominee or other intermediary. If so, a necessary precondition is receipt of satisfactory evidence of the identity of any intermediaries, and of the persons upon whose behalf they are acting, as well as details of the nature of the trust or other arrangements in place. Specifically, the identification of a trust should include the trustees, settlors/grantors and beneficiaries[140].

2.2.2 Corporate vehicles

33. Banks need to be vigilant in preventing corporate business entities from being used by natural persons as a method of operating anonymous accounts. Personal asset holding vehicles, such as international business companies, may make proper identification of customers or beneficial owners

---

[138] Subject to any national legislation concerning handling of suspicious transactions.

[139] In a numbered account, the name of the beneficial owner is known to the bank but is substituted by an account number or code name in subsequent documentation.

[140] Beneficiaries should be identified as far as possible when defined. It is recognised that it may not be possible to identify the beneficiaries of trusts precisely at the outset. For example, some beneficiaries may be unborn children and some may be conditional on the occurrence of specific events. In addition, beneficiaries being specific classes of individuals (e.g. employee pension funds) may be appropriately dealt with as pooled accounts as referred to in paragraphs 38-9.

difficult. A bank should understand the structure of the company, determine the source of funds, and identify the beneficial owners and those who have control over the funds.

34. Special care needs to be exercised in initiating business transactions with companies that have nominee shareholders or shares in bearer form. Satisfactory evidence of the identity of beneficial owners of all such companies needs to be obtained. In the case of entities which have a significant proportion of capital in the form of bearer shares, extra vigilance is called for. A bank may be completely unaware that the bearer shares have changed hands. The onus is on banks to put in place satisfactory procedures to monitor the identity of material beneficial owners. This may require the bank to immobilise the shares, e.g. by holding the bearer shares in custody.

2.2.3 Introduced business

35. The performance of identification procedures can be time consuming and there is a natural desire to limit any inconvenience for new customers. In some countries, it has therefore become customary for banks to rely on the procedures undertaken by other banks or introducers when business is being referred. In doing so, banks risk placing excessive reliance on the due diligence procedures that they expect the introducers to have performed. Relying on due diligence conducted by an introducer, however reputable, does not in any way remove the ultimate responsibility of the recipient bank to know its customers and their business. In particular, banks should not rely on introducers that are subject to weaker standards than those governing the banks' own KYC procedures or that are unwilling to share copies of due diligence documentation.

36. The Basel Committee recommends that banks that use introducers should carefully assess whether the introducers are "fit and proper" and are exercising the necessary due diligence in accordance with the standards set out in this paper. The ultimate responsibility for knowing customers always lies with the bank. Banks should use the following criteria to determine whether an introducer can be relied upon:[141]

- it must comply with the minimum customer due diligence practices identified in this paper;
- the customer due diligence procedures of the introducer should be as rigorous as those which the bank would have conducted itself for the customer;
- the bank must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer;
- the bank must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage; and
- all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the bank, who must carefully review the documentation provided. Such information must be available for review by the supervisor and the financial intelligence unit or equivalent enforcement agency, where appropriate legal authority has been obtained.

In addition, banks should conduct periodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above.

2.2.4 Client accounts opened by professional intermediaries

[141] The FATF is currently engaged in a review of the appropriateness of eligible introducers.

37. When a bank has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified.

38. Banks often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds and money funds. Banks also hold pooled accounts managed by lawyers or stockbrokers that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the bank, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified.

39. Where the funds are co-mingled, the bank should look through to the beneficial owners. There can be circumstances where the bank may not need to look beyond the intermediary, for example, when the intermediary is subject to the same regulatory and money laundering legislation and procedures, and in particular is subject to the same due diligence standards in respect of its client base as the bank. National supervisory guidance should clearly set out those circumstances in which banks need not look beyond the intermediary. Banks should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. In assessing the due diligence process of the intermediary, the bank should apply the criteria set out in paragraph 36 above, in respect of introduced business, in order to determine whether a professional intermediary can be relied upon.

40. Where the intermediary is not empowered to furnish the required information on beneficiaries to the bank, for example, lawyers[142] bound by professional secrecy codes or when that intermediary is not subject to due diligence standards equivalent to those set out in this paper or to the requirements of comprehensive anti-money laundering legislation, then the bank should not permit the intermediary to open an account.

2.2.5 Politically exposed persons

41. Business relationships with individuals holding important public positions and with persons or companies clearly related to them may expose a bank to significant reputational and/or legal risks. Such politically exposed persons ("PEPs") are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of publicly owned corporations and important political party officials. There is always a possibility, especially in countries where corruption is widespread, that such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, etc.

42. Accepting and managing funds from corrupt PEPs will severely damage the bank's own reputation and can undermine public confidence in the ethical standards of an entire financial centre, since such cases usually receive extensive media attention and strong political reaction, even if the illegal origin of the assets is often difficult to prove. In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

43. Some countries have recently amended or are in the process of amending their laws

[142] The FATF is currently engaged in a review of KYC procedures governing accounts opened by lawyers on behalf of clients.

and regulations to criminalise active corruption of foreign civil servants and public officers in accordance with the relevant international convention.[143] In these jurisdictions foreign corruption becomes a predicate offence for money laundering and all the relevant anti-money laundering laws and regulations apply (e.g. reporting of suspicious transactions, prohibition on informing the customer, internal freeze of funds etc). But even in the absence of such an explicit legal basis in criminal law, it is clearly undesirable, unethical and incompatible with the fit and proper conduct of banking operations to accept or maintain a business relationship if the bank knows or must assume that the funds derive from corruption or misuse of public assets. There is a compelling need for a bank considering a relationship with a person whom it suspects of being a PEP to identify that person fully, as well as people and companies that are clearly related to him/her.

44. Banks should gather sufficient information from a new customer, and check publicly available information, in order to establish whether or not the customer is a PEP. Banks should investigate the source of funds before accepting a PEP. The decision to open an account for a PEP should be taken at a senior management level.

2.2.6 Non-face-to-face customers

45. Banks are increasingly asked to open accounts on behalf of customers who do not present themselves for personal interview. This has always been a frequent event in the case of non-resident customers, but it has increased significantly with the recent expansion of postal, telephone and electronic banking. Banks should apply equally effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those available for interview. One issue that has arisen in this connection is the possibility of independent verification by a reputable third party. This whole subject of nonface- to-face customer identification is being discussed by the FATF, and is also under review in the context of amending the 1991 EEC Directive.

46. A typical example of a non-face-to-face customer is one who wishes to conduct electronic banking via the Internet or similar technology. Electronic banking currently incorporates a wide array of products and services delivered over telecommunications networks. The impersonal and borderless nature of electronic banking combined with the speed of the transaction inevitably creates difficulty in customer identification and verification. As a basic policy, supervisors expect that banks should proactively assess various risks posed by emerging technologies and design customer identification procedures with due regard to such risks.'[15]

47. Even though the same documentation can be provided by face-to-face and nonface-to-face customers, there is a greater difficulty in matching the customer with the documentation in the case of non-face-to-face customers. With telephone and electronic banking, the verification problem is made even more difficult.

48. In accepting business from non-face-to-face customers:

- banks should apply equally effective customer identification procedures for nonface-
- to-face customers as for those available for interview; and
- there must be specific and adequate measures to mitigate the higher risk.

---

[143] See OECD Convention on *Combating Bribery of Foreign Public Officials in International Business Transactions*, adopted by the Negotiating Conference on 21 November 1997.

[15] The Electronic Banking Group of the Basel Committee issued a paper on risk management principles for electronic banking in May 2001.

Examples of measures to mitigate risk include:

- certification of documents presented;
- requisition of additional documents to complement those which are required for face-to-face customers;
- independent contact with the customer by the bank;
- third party introduction, e.g. by an introducer subject to the criteria established in paragraph 36; or
- requiring the first payment to be carried out through an account in the customer's name with another bank subject to similar customer due diligence standards.

2.2.7 Correspondent banking

49. Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Used by banks throughout the world, correspondent accounts enable banks to conduct business and provide services that the banks do not offer directly. Correspondent accounts that merit particular care involve the provision of services in jurisdictions where the respondent banks have no physical presence. However, if banks fail to apply an appropriate level of due diligence to such accounts, they expose themselves to the range of risks identified earlier in this paper, and may find themselves holding and/or transmitting money linked to corruption, fraud or other illegal activity.

50. Banks should gather sufficient information about their respondent banks to understand fully the nature of the respondent's business. Factors to consider include: information about the respondent bank's management, major business activities, where they are located and its money-laundering prevention and detection efforts; the purpose of the account; the identity of any third party entities that will use the correspondent banking services; and the condition of bank regulation and supervision in the respondent's country.

Banks should only establish correspondent relationships with foreign banks that are effectively supervised by the relevant authorities. For their part, respondent banks should have effective customer acceptance and KYC policies.

51. In particular, banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks). Banks should pay particular attention when continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified as being "noncooperative" in the fight against anti-money laundering. Banks should establish that their respondent banks have due diligence standards as set out in this paper, and employ enhanced due diligence procedures with respect to transactions carried out though the correspondent accounts.

52. Banks should be particularly alert to the risk that correspondent accounts might be used directly by third parties to transact business on their own behalf (e.g. payable-through accounts). Such arrangements give rise to most of the same considerations applicable to introduced business and should be treated in accordance with the criteria set out in paragraph 36.

3. On-going monitoring of accounts and transactions

53. On-going monitoring is an essential aspect of effective KYC procedures. Banks can

only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account's activity. Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so. The extent of the monitoring needs to be risk-sensitive. For all accounts, banks should have systems in place to detect unusual or suspicious patterns of activity. This can be done by establishing limits for a particular class or category of accounts. Particular attention should be paid to transactions that exceed these limits. Certain types of transactions should alert banks to the possibility that the customer is conducting unusual or suspicious activities. They may include transactions that do not appear to make economic or commercial sense, or that involve large amounts of cash deposits that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "washed" through the account. Examples of suspicious activities can be very helpful to banks and should be included as part of a jurisdiction's anti-money laundering procedures and/or guidance.

54. There should be intensified monitoring for higher risk accounts. Every bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors. For higher risk accounts:

Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyse and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.

Senior management in charge of private banking business should know the personal circumstances of the bank's high risk customers and be alert to sources of third party information. Significant transactions by these customers should be approved by a senior manager.

Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them.[145] As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.

4. Risk management

55. Effective KYC procedures embrace routines for proper management oversight, systems and controls, segregation of duties, training and other related policies. The board of directors of the bank should be fully committed to an effective KYC programme by establishing appropriate procedures and ensuring their effectiveness. Explicit responsibility should be allocated within the bank for ensuring that the bank's policies and procedures are managed effectively and are, at a minimum, in accordance with local supervisory practice.

[145] It is unrealistic to expect the bank to know or investigate every distant family, political or business connection of a foreign customer. The need to pursue suspicions will depend on the size of the assets or turnover, pattern of transactions, economic background, reputation of the country, plausibility of the customer's explanations etc. It should however be noted that PEPs (or rather their family members and friends) would not necessarily present themselves in that capacity, but rather as ordinary (albeit wealthy) business people, masking the fact they owe their high position in a legitimate business corporation only to their privileged relation with the holder of the public office.

The channels for reporting suspicious transactions should be clearly specified in writing, and communicated to all personnel. There should also be internal procedures for assessing whether the bank's statutory obligations under recognised suspicious activity reporting regimes require the transaction to be reported to the appropriate law enforcement and and/or supervisory authorities.
56. Banks' internal audit and compliance functions have important responsibilities in evaluating and ensuring adherence to KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Its responsibilities should include ongoing monitoring of staff performance through sample testing of compliance and review of exception reports to alert senior management or the Board of Directors if it believes management is failing to address KYC procedures in a responsible manner.

57. Internal audit plays an important role in independently evaluating the risk management and controls, discharging its responsibility to the Audit Committee of the Board of Directors or a similar oversight body through periodic evaluations of the effectiveness of compliance with KYC policies and procedures, including related staff training. Management should ensure that audit functions are staffed adequately with individuals who are well versed in such policies and procedures. In addition, internal auditors should be proactive in following-up their findings and criticisms.

58. All banks must have an ongoing employee-training programme so that bank staff are adequately trained in KYC procedures. The timing and content of training for various sectors of staff will need to be adapted by the bank for its own needs. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new customers. New staff should be educated in the importance of KYC policies and the basic requirements at the bank. Front-line staff members who deal directly with the public should be trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an ongoing basis and to detect patterns of suspicious activity. Regular refresher training should be provided to ensure that staff are reminded of their responsibilities and are kept informed of new developments. It is crucial that all relevant staff fully understand the need for and implement KYC policies consistently. A culture within banks that promotes such understanding is the key to successful implementation.

59. In many countries, external auditors also have an important role to play in monitoring banks' internal controls and procedures, and in confirming that they are in compliance with supervisory practice.

IV. The role of supervisors

60. Based on existing international KYC standards, national supervisors are expected to set out supervisory practice governing banks' KYC programmes. The essential elements as presented in this paper should provide clear guidance for supervisors to proceed with the work of designing or improving national supervisory practice.

61. In addition to setting out the basic elements for banks to follow, supervisors have a responsibility to monitor that banks are applying sound KYC procedures and are sustaining ethical and professional standards on a continuous basis. Supervisors should ensure that appropriate internal controls are in place and that banks are in compliance with supervisory and regulatory guidance. The supervisory process should include not only a review of policies and procedures but also a review of customer files and the sampling of some accounts. Supervisors should always have the right to access all documentation related to accounts maintained in that jurisdiction, including any analysis the bank has made to detect unusual or suspicious transactions.

62. Supervisors have a duty not only to ensure their banks maintain high KYC standards

to protect their own safety and soundness but also to protect the integrity of their national banking system.[146] Supervisors should make it clear that they will take appropriate action, which may be severe and public if the circumstances warrant, against banks and their officers who demonstrably fail to follow their own internal procedures and regulatory requirements. In addition, supervisors should ensure that banks are aware of and pay particular attention to transactions that involve jurisdictions where standards are considered inadequate. The FATF and some national authorities have listed a number of countries and jurisdictions that are considered to have legal and administrative arrangements that do not comply with international standards for combating money laundering. Such findings should be a component of a bank's KYC policies and procedures.

V. Implementation of KYC standards in a cross-border context

63. Supervisors around the world should seek, to the best of their efforts, to develop and implement their national KYC standards fully in line with international standards so as to avoid potential regulatory arbitrage and safeguard the integrity of domestic and international banking systems. The implementation and assessment of such standards put to the test the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a groupwide basis. This is a challenging task for banks and supervisors alike.

64. Supervisors expect banking groups to apply an accepted minimum standard of KYC policies and procedures to both their local and overseas operations. The supervision of international banking can only be effectively carried out on a consolidated basis, and reputational risk as well as other banking risks are not limited to national boundaries. Parent banks must communicate their policies and procedures to their overseas branches and subsidiaries, including non-banking entities such as trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programmes to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Therefore, it is important that KYC documentation is properly filed and available for their inspection. As far as compliance checks are concerned, supervisors and external auditors should in most cases examine systems and controls and look at customer accounts and transactions monitoring as part of a sampling process.

65. However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

66. Where the minimum KYC standards of the home and host countries differ, branches and subsidiaries in the host jurisdictions should apply the higher standard of the two. In general, there should be no impediment to prevent a bank from adopting standards that are higher than the minima required locally. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of home country KYC standards, where the latter are more stringent, host country supervisors should use their best endeavours to have the law and regulations changed. In the meantime, overseas branches and subsidiaries would have to comply with host country standards, but they should make sure the head office or parent bank and its home country supervisor are fully informed of the nature of the difference.

67. Criminal elements are likely to be drawn toward jurisdictions with such impediments.

---

[146] Many supervisors also have a duty to report any suspicious, unusual or illegal transactions that they detect, for example, during onsite examinations.

Hence, banks should be aware of the high reputational risk of conducting business in these jurisdictions. Parent banks should have a procedure for reviewing the vulnerability of the individual operating units and implement additional safeguards where appropriate. In extreme cases, supervisors should consider placing additional controls on banks operating in those jurisdictions and ultimately perhaps encouraging their withdrawal.

68. During on-site inspections, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. This will require a review of customer files and some random sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices, and should not be impeded by local bank secrecy laws. Where the home country supervisor requires consolidated reporting of deposit or borrower concentrations or notification of funds under management, there should be no impediments. In addition, with a view to monitoring deposit concentrations or the funding risk of the deposit being withdrawn, home supervisors may apply materiality tests and establish some thresholds so that if a customer's deposit exceeds a certain percentage of the balance sheet, banks should report it to the home supervisor. However, safeguards are needed to ensure that information regarding individual accounts is used exclusively for lawful supervisory purposes, and can be protected by the recipient in a satisfactory manner. A statement of mutual cooperation[147] to facilitate information sharing between the two supervisors would be helpful in this regard.

69. In certain cases there may be a serious conflict between the KYC policies of a parent bank imposed by its home authority and what is permitted in a cross-border office. There may, for example, be local laws that prevent inspections by the parent banks' compliance officers, internal auditors or home country supervisors, or that enable bank customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are. In such cases, the home supervisor should communicate with the host supervisor in order to confirm whether there are indeed genuine legal impediments and whether they apply extraterritorially. If they prove to be insurmountable, and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the bank may decide for itself, or be required by its home supervisor, to close down the operation in question. In the final analysis, any arrangements underpinning such on-site examinations should provide a mechanism that permits an assessment that is satisfactory to the home supervisor. Statements of cooperation or memoranda of understanding setting out the mechanics of the arrangements may be helpful. Access to information by home country supervisors should be as unrestricted as possible, and at a minimum they should have free access to the banks' general policies and procedures for customer due diligence and for dealing with suspicions.

[147] See the Basel Committee paper *Essential elements of a statement of cooperation between banking supervisors* (May 2001).

Excerpts from *Core Principles Methodology*

Principle 15: Banking supervisors must determine that banks have adequate policies, practices and procedures in place, including strict "know-your-customer" rules, that promote high ethical and professional standards in the financial sector and prevent the bank being used, intentionally or unintentionally, by criminal elements.

Essential criteria

1. The supervisor determines that banks have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the bank from being used, intentionally or unintentionally, by criminal elements. This includes the prevention and detection of criminal activity or fraud, and reporting of such suspected activities to the appropriate authorities.

2. The supervisor determines that banks have documented and enforced policies for identification of customers and those acting on their behalf as part of their antimoney-laundering program. There are clear rules on what records must be kept on customer identification and individual transactions and the retention period.

3. The supervisor determines that banks have formal procedures to recognise potentially suspicious transactions. These might include additional authorisation for large cash (or similar) deposits or withdrawals and special procedures for unusual transactions.

4. The supervisor determines that banks appoint a senior officer with explicit responsibility for ensuring that the bank's policies and procedures are, at a minimum, in accordance with local statutory and regulatory anti-money laundering requirements.

5. The supervisor determines that banks have clear procedures, communicated to all personnel, for staff to report suspicious transactions to the dedicated senior officer responsible for anti-money laundering compliance.

6. The supervisor determines that banks have established lines of communication both to management and to an internal security (guardian) function for reporting problems.

7. In addition to reporting to the appropriate criminal authorities, banks report to the supervisor suspicious activities and incidents of fraud material to the safety, soundness or reputation of the bank.

8. Laws, regulations and/or banks' policies ensure that a member of staff who reports suspicious transactions in good faith to the dedicated senior officer, internal security function, or directly to the relevant authority cannot be held liable.

9. The supervisor periodically checks that banks' money laundering controls and their systems for preventing, identifying and reporting fraud are sufficient. The supervisor has adequate enforcement powers (regulatory and/or criminal prosecution) to take

action against a bank that does not comply with its anti-money laundering obligations.

10. The supervisor is able, directly or indirectly, to share with domestic and foreign

financial sector supervisory authorities information related to suspected or actual criminal activities.

11. The supervisor determines that banks have a policy statement on ethics and professional behaviour that is clearly communicated to all staff.

Additional criteria

1. The laws and/or regulations embody international sound practices, such as compliance with the relevant forty Financial Action Task Force Recommendations issued in 1990 (revised 1996).

2. The supervisor determines that bank staff is adequately trained on money laundering detection and prevention.

3. The supervisor has the legal obligation to inform the relevant criminal authorities of any suspicious transactions.

4. The supervisor is able, directly or indirectly, to share with relevant judicial authorities information related to suspected or actual criminal activities.

5. If not performed by another agency, the supervisor has in-house resources with specialist expertise on financial fraud and anti-money laundering obligations.

Annex 4

COMBATING THE ABUSE OF NON-PROFIT ORGANISATIONS

International Best Practices

Introduction and definition

1. The misuse of non-profit organisations for the financing of terrorism is coming to be recognised as a crucial weak point in the global struggle to stop such funding at its source. This issue has captured the attention of the Financial Action Task Force (FATF), the G7, and the United Nations, as well as national authorities in many regions. Within the FATF, this has rightly become the priority focus of work to implement Special Recommendation VIII (Non-profit organisations).

2. Non-profit organisations can take on a variety of forms, depending on the jurisdiction and legal system. Within FATF members, law and practice recognise associations, foundations, fundraising committees, community service organisations, corporations of public interest, limited companies, Public Benevolent Institutions, all as legitimate forms of non-profit organisation, just to name a few.

3. This variety of legal forms, as well as the adoption of a risk-based approach to the problem, militates in favour of a functional, rather than a legalistic definition. Accordingly, the FATF has developed suggested practices that would best aid authorities to protect non-profit organisations **that engage in raising or disbursing funds** for charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works" from being misused or exploited by the financiers of terrorism.

Statement of the Problem

4. Unfortunately, numerous instances have come to light in which the mechanism of charitable fundraising – *i.e.*, the collection of resources from donors and its redistribution for charitable purposes– has been used to provide a cover for the financing of terror. In certain cases, the organisation itself was a mere sham that existed simply to funnel money to terrorists. However, often the abuse of nonprofit organisations occurred without the knowledge of donors, or even of members of the management and staff of the organisation itself, due to malfeasance by employees and/or managers diverting funding on their own. Besides financial support, some non-profit organisations have also provided cover and logistical support for the movement of terrorists and illicit arms. Some examples of these kinds of activities were presented in the 2001-2002 FATF Report on Money Laundering Typologies[148]; others are presented in the annex to this paper.

Principles

5. The following principles guide the establishment of these best practices:

- The charitable sector is a vital component of the world economy and of many national economies and social systems that complements the activity of the governmental and business sectors in supplying a broad spectrum of public services and improving quality of life. We wish to safeguard and maintain the practice of charitable giving and the strong and diversified community of institutions through which it operates.

- Oversight of non-profit organisations is a co-operative undertaking among government, the charitable community, persons who support charity, and those whom it serves. Robust oversight mechanisms

[148] Published February 2002 and available at http://www.fatf-gafi.org/FATDocs_en.htm#Trends.

and a degree of institutional tension between non-profit organisations and government entities charged with their oversight do not preclude shared goals and complementary functions – both seek to promote transparency and accountability and, more broadly, common social welfare and security goals.

- Government oversight should be flexible, effective, and proportional to the risk of abuse. Mechanisms that reduce the compliance burden without creating loopholes for terrorist financiers should be given due consideration. Small organisations that do not raise significant amounts of money from public sources, and locally based associations or organisations whose primary function is to redistribute resources among members may not necessarily require enhanced government oversight.

- Different jurisdictions approach the regulation of non-profit organisations from different constitutional, legal, regulatory, and institutional frameworks, and any international standards or range of models must allow for such differences, while adhering to the goals of establishing transparency and accountability in the ways in which non-profit organisations collect and transmit funds. It is understood as well that jurisdictions may be restricted in their ability to regulate religious activity.

- Jurisdictions may differ on the scope of purposes and activities that are within the definition of "charity," but all should agree that it does not include activities that directly or indirectly support terrorism, including actions that could serve to induce or compensate for participation in terrorist acts.

- The non-profit sector in many jurisdictions has representational, self-regulatory, watchdog, and accreditation organisations that can and should play a role in the protection of the sector against abuse, in the context of a public-private partnership. Measures to strengthen self-regulation should be encouraged as a significant method of decreasing the risk of misuse by terrorist groups.

Areas of focus

6. Preliminary analysis of the investigations, blocking actions, and law-enforcement activities of various jurisdictions indicate several ways in which non-profit organisations have been misused by terrorists and suggests areas in which preventive measures should be considered.

(i) Financial transparency

7. Non-profit organisations collect hundreds of billions of dollars annually from donors and distribute those monies – after paying for their own administrative costs – to beneficiaries. Transparency is in the interest of the donors, organisations, and authorities. However, the sheer volume of transactions conducted by non-profit organisations combined with the desire not to unduly burden legitimate organisations generally underscore the importance of risk and size-based proportionality in setting the appropriate level of rules and oversight in this area.

a. Financial accounting

- Non-profit organisations should maintain and be able to present full program budgets that account for all programme expenses. These budgets should indicate the identity of recipients and how the money is to be used. The administrative budget should also be protected from diversion through similar oversight, reporting, and safeguards.

- Independent auditing is a widely recognised method of ensuring that that accounts of an organisation accurately reflect the reality of its finances and should be considered a best practice. Many major non-profit organisations undergo audits to retain donor confidence, and regulatory authorities in some jurisdictions require them for non-profit organisations. Where practical, such audits should be conducted to ensure that such organisations are not being abused by terrorist groups. It should be

noted that such financial auditing is not a guarantee that program funds are actually reaching the intended beneficiaries.

b. Bank accounts:

- It is considered a best practice for non-profit organisations that handle funds to maintain registered bank accounts, keep its funds in them, and utilise formal or registered financial channels for transferring funds, especially overseas. Where feasible, therefore, non-profit organisations that handle large amounts of money should use formal financial systems to conduct their financial transactions. Adoption of this best practice would bring the accounts of non-profit organisations, by and large, within the formal banking system and under the relevant controls or regulations of that system.

(ii) Programmatic verification

8. The need to verify adequately the activities of a non-profit organisation is critical. In several instances, programmes that were reported to the home office were not being implemented as represented. The funds were in fact being diverted to terrorist organisations. Non-profit organizations should be in a position to know and to verify that funds have been spent as advertised and planned.

a. Solicitations

9. Solicitations for donations should accurately and transparently tell donors the purpose(s) for which donations are being collected. The non-profit organisation should then ensure that such funds are used for the purpose stated.

b. Oversight

10. To help ensure that funds are reaching the intended beneficiary, non-profit organizations should ask following general questions:

- Have projects actually been carried out?
- Are the beneficiaries real?
- Have the intended beneficiaries received the funds that were sent for them?
- Are all funds, assets, and premises accounted for?

c. Field examinations

11. In several instances, financial accounting and auditing might be insufficient protection against the abuse of non-profit organisations. Direct field audits of programmes may be, in some instances, the only method for detecting misdirection of funds. Examination of field operations is clearly a superior mechanism for discovering malfeasance of all kinds, including diversion of funds to terrorists. Given considerations of risk-based proportionality, across-the-board examination of all programmes would not be required. However, non-profit organisations should track programme accomplishments as well as finances. Where warranted, examinations to verify reports should be conducted.

d. Foreign operations

12. When the home office of the non-profit organisation is in one country and the beneficent operations take place in another, the competent authorities of both jurisdictions should strive to exchange information and co-ordinate oversight or investigative work, in accordance with their comparative advantages. Where possible, a non-profit organisation should take appropriate measures to account for funds and services delivered in locations other than in its home jurisdiction.

(iii) Administration

13. Non-profit organisations should be able to document their administrative, managerial, and policy control over their operations. The role of the Board of Directors, or its equivalent, is key.

14. Much has been written about the responsibilities of Boards of Directors in the corporate world and recent years have seen an increased focus and scrutiny of the important role of the Directors in the healthy and ethical functioning of the corporation. Directors of non-profit organisations, or those with equivalent responsibility for the direction and control of an organisation's management, likewise have a responsibility to act with due diligence and a concern that the organisation operates ethically. The directors or those exercising ultimate control over a non-profit organisation need to know who is acting in the organisation's name – in particular, responsible parties such as office directors, plenipotentiaries, those with signing authority and fiduciaries. Directors should exercise care, taking proactive verification measures whenever feasible, to ensure their partner organisations and those to which they provide funding, services, or material support, are not being penetrated or manipulated by terrorists.

15. Directors should act with diligence and probity in carrying out their duties. Lack of knowledge or passive involvement in the organisation's affairs does not absolve a director – or one who controls the activities or budget of a non-profit organisation – of responsibility. To this end, directors have responsibilities to:

- The organisation and its members to ensure the financial health of the organisation and that it focuses on its stated mandate.
- Those with whom the organisation interacts, like donors, clients, suppliers.
- All levels of government that in any way regulate the organisation.

16. These responsibilities take on new meaning in light of the potential abuse of non-for-profit organisations for terrorist financing. If a non-profit organisation has a board of directors, the board of directors should:

- Be able to identify positively each board and executive member;
- Meet on a regular basis, keep records of the decisions taken at these meetings and through these meetings;
- Formalise the manner in which elections to the board are conducted as well as the manner in which a director can be removed;
- Ensure that there is an annual independent review of the finances and accounts of the

organisation;
- Ensure that there are appropriate financial controls over program spending, including programs undertaken through agreements with other organisations;
- Ensure an appropriate balance between spending on direct programme delivery and administration;
- Ensure that procedures are put in place to prevent the use of the organisation's facilities or assets to support or condone terrorist activities.

Oversight bodies

17. Various bodies in different jurisdictions interact with the charitable community. In general, preventing misuse of non-profit organisations or fundraising organisations by terrorists has not been a historical focus of their work. Rather, the thrust of oversight, regulation, and accreditation to date has been maintaining donor confidence through combating waste and fraud, as well as ensuring that government tax relief benefits, where applicable, go to appropriate organisations. While much of this oversight focus is fairly easily transferable to the fight against terrorist finance, this will also require a broadening of focus.

18. There is not a single correct approach to ensuring appropriate transparency within non-profit organisations, and different jurisdictions use different methods to achieve this end. In some, independent charity commissions have an oversight role, in other jurisdictions government ministries are directly involved, just to take two examples. Tax authorities play a role in some jurisdictions, but not in others. Other authorities that have roles to play in the fight against terrorist finance include law enforcement agencies and bank regulators. Far from all the bodies are governmental – private sector watchdog or accreditation organisations play an important role in many jurisdictions.

(i) Government Law Enforcement and Security officials

19. Non-profit organisations funding terrorism are operating illegally, just like any other illicit financier; therefore, much of the fight against the abuse of non-profit organisations will continue to rely heavily on law enforcement and security officials. Non-profit organisations are not exempt from the criminal laws that apply to individuals or business enterprises.

- Law enforcement and security officials should continue to play a key role in the combat against the abuse of non-profit organisations by terrorist groups, including by continuing their ongoing activities with regard to non-profit organisations.

(ii) Specialised Government Regulatory Bodies

20. A brief overview of the pattern of specialised government regulation of non-profit organisations shows a great variety of practice. In England and Wales, such regulation is housed in a special Charities Commission. In the United States, any specialised government regulation occurs at the sub-national (state) level. GCC member countries oversee non-profit organisations with a variety of regulatory bodies, including government ministerial and intergovernmental agencies.

- In all cases, there should be interagency outreach and discussion within governments on the issue of terrorist financing – especially between those agencies that have traditionally dealt with terrorism and regulatory bodies that may not be aware of the terrorist financing risk to non-profit organisations. Specifically, terrorist financing experts should work with non-profit organization oversight authorities to raise awareness of the problem, and they should alert these authorities to the specific characteristics of terrorist financing.

(iii) Government Bank, Tax, and Financial Regulatory Authorities

21. While bank regulators are not usually engaged in the oversight of non-profit organisations, the earlier discussion of the importance of requiring charitable fund-raising and transfer of funds to go through formal or

registered channels underscores the benefit of enlisting the established powers of the bank regulatory system – suspicious activity reporting, know-your-customer (KYC) rules, etc – in the fight against terrorist abuse or exploitation of non-profit organisations.

22. In those jurisdictions that provide tax benefits to charities, tax authorities have a high level of interaction with the charitable community. This expertise is of special importance to the fight against terrorist finance, since it tends to focus on the financial workings of charities.

- Jurisdictions which collect financial information on charities for the purposes of tax deductions should encourage the sharing of such information with government bodies involved in the combating of terrorism (including FIUs) to the maximum extent possible. Though such tax-related information may be sensitive, authorities should ensure that information relevant to the misuse of non-profit organisations by terrorist groups or supporters is shared as appropriate.

(iv) Private Sector Watchdog Organisations

23. In the countries and jurisdictions where they exist, the private sector watchdog or accreditation organisations are a unique resource that should be a focal point of international efforts to combat the abuse of non-profit organisations by terrorists. Not only do they contain observers knowledgeable of fundraising organisations, they are also very directly interested in preserving the legitimacy and reputation of the non-profit organisations. More than any other class of participants, they have long been engaged in the development and promulgation of "best practices" for these organisations in a wide array of functions.

24. Jurisdictions should make every effort to reach out and engage such watchdog and accreditation organisations in their attempt to put best practices into place for combating the misuse of non-profit organisations. Such engagement could include a dialogue on how to improve such practices.

Sanctions

25. Countries should use existing laws and regulations or establish any such new laws or regulations to establish effective and proportionate administrative, civil, or criminal penalties for those who misuse charities for terrorist financing.

TYPOLOGIES OF TERRORIST MISUSE OF NON-PROFIT ORGANISATIONS

Annex

Example 1: Non-profit front organisation

1. In 1996, a number of individuals known to belong to the religious extremist groups established in the south-east of an FATF country (Country A) convinced wealthy foreign nationals, living for unspecified reasons in Country A, to finance the construction of a place of worship. These wealthy individuals were suspected of assisting in the concealment of part of the activities of a terrorist group. It was later established that "S", a businessman in the building sector, had bought the building intended to house the place of worship and had renovated it using funds from one of his companies. He then transferred the ownership of this building, for a large profit, to Group Y belonging to the wealthy foreigners mentioned above.

2. This place of worship intended for the local community in fact also served as a place to lodge clandestine "travellers" from extremist circles and collect funds. For example, soon after the work was completed, it was noticed that the place of worship was receiving large donations (millions of dollars) from other wealthy foreign businessmen. Moreover, a Group Y worker was said to have convinced his employers that a "foundation" would be more suitable for collecting and using large funds without attracting the attention of local authorities. A foundation was thus reportedly established for this purpose.

3. It is also believed that part of "S's" activities in heading a multipurpose international financial network (for which investments allegedly stood at USD 53 million for Country A in 1999 alone) was to provide support to a terrorist network. "S" had made a number of trips to Afghanistan and the United States. Amongst his assets were several companies registered in Country C and elsewhere. One of these companies, located in the capital of Country A, was allegedly a platform for collecting funds. "S" also purchased several buildings in the south of Country A with the potential collusion of a notary and a financial institution.

4. When the authorities of Country A blocked a property transaction on the basis of the foreign investment regulations, the financial institution's director stepped in to support his client's transaction and the notary presented a purchase document for the building thus ensuring that the relevant authorisation was delivered. The funds held by the bank were then transferred to another account in a bank in an NCCT jurisdiction to conceal their origin when they were used in Country A.

5. Even though a formal link has not as yet been established between the more or less legal activities of the parties in Country A and abroad and the financing of terrorist activities carried out under the authority a specific terrorist network, the investigators suspect that at least part of the proceeds from these activities have been used for this purpose.

Example 2: Fraudulent solicitation of donations

6. One non-profit organisation solicited donations from local charities in a donor region, in addition to fund raising efforts conducted at its headquarters in a beneficiary region. This non-profit organisation falsely asserted that the funds collected were destined for orphans and widows. In fact, the finance chief of this organisation served as the head of organised fundraising for Usama bin Laden. Rather than providing support for orphans and widows, funds collected by the non-profit organisation were turned over to al-Qaida operatives.

Example 3: Branch offices defraud headquarters

7. The office director for a non-profit organisation in a beneficiary region defrauded donors from a donor region to fund terrorism. In order to obtain additional funds from the headquarters, the branch office

padded the number of orphans it claimed to care for by providing names of orphans that did not exist or who had died. Funds then sent for the purpose of caring for the non-existent or dead orphans were instead diverted to al-Qaida terrorists.

8. In addition, the branch office in a beneficiary region of another non-profit organisation based in a donor region provided a means of funnelling money to a known local terrorist organisation by disguising funds as intended to be used for orphanage projects or the construction of schools and houses of worship. The office also employed members of the terrorist organisations and facilitated their travel.

Example 4: Aid worker's Misuse of Position

9. An employee working for an aid organisation in a war-ravaged region used his employment to support the ongoing activities of a known terrorist organisation from another region. While working for the aid organisation as a monitor for work funded in that region, the employee secretly made contact with weapons smugglers in the region. He used his position as cover as he brokered the purchase and export of weapons to the terrorist organisation.

Annex 5

1981 Regulations Regarding Associations and Charitable Institutions

I. STEPS NECESSARY TO OPEN A CHARITY
- a. 20 or more individuals are necessary to open a charity.
- b. All members must have no criminal record.
- c. Permission is required from Ministry of Labor and Social Affairs (MLSA)
- d. Charities must register with the MLSA.
- e. Once a charity receives authorization from MLSA, the board of directors of the charity must make an official announcement in the government circular.
- f. A charity must announce the names of the board of directors, the organization chart and the goals of organization.

II. DEFINITION OF CHARITY

Provides social services in money or kind, for education and health without gaining financial profit. Charities are forbidden from making money.

III. SUBSIDIARY INFO
- a. Charities cannot open subsidiaries without the permission of MLSA.
- b. Changes in organization chart should be forwarded to MLSA for authorization.

IV. THE MLSA LICENSES CHARITIES
- a. The license contains date of registration
- b. The license give each charity an identification number.
- c. The date the registration was announced in the official record.
- d. The license includes the address of charity.

V. ORGANIZATION CHART SHOULD INCLUDE THE FOLLOWING:
- a. The name of the charity, official address and jurisdiction.
- b. The goals of the charity.
- c. The name, age, personal address of the founding members.
- d. Requirements necessary for membership.
- e. Budget and allocations of finances.
- f. The fiscal operating year.
- g. Internal financial controls.
- h. Information about subsidiaries, their missions and goals the necessary requirements to be a subsidiary. Rules of termination of partnership with subsidiaries and parent.
- i. Conditions and rules to change or amend the organization,
- j. Rules for dissolving of charity and outcome of remaining proceeds.
- k. Proceeds after dissolving charity must go to another registered charity.

VI MISCELLANEOUS

VII. DEFINITION OF PUBLIC ASSOCIATION
- a. An association must be in existence for one year with all of its members having paid their dues prior to being considered an association.
- b. The public association must hold all its meeting in its official address except with prior approval from MLSA. The rules, invitation, agenda and procedures of the meeting must be published in advanced.
- c. MLSA must be notified 15 days prior to meeting with copy of the agenda.

VIII. SELECTION OF BOARD OF DIRECTORS
- a. Election must be done by secret ballot, with a MLSA representative present at the election.

b. Board of directors have 4 years term limits.
c. 90 days prior to election the MLSA must receive a list of candidates, if after 60 days the association has not heard anything from the MLSA then this implies approval of candidate. The MLSA representative can nullify the results of the election due to cause up to 15 days after the election.
d. Within 10 days of every meeting the minutes must be sent to MLSA, the MLSA has 20 days to block the actions detailed in the minutes.
e. By-laws for meetings must be established.

IX. THE INTERIM BOARD OF DIRECTORS.

MLSA can appoint an interim board of directors if the MLSA thinks it serves in the best interest of the association.

X. The board of directors must submit all financial statements to the MLSA and an operating budget and pro-forma budget signed by president or vice president, treasurer, accountant, an auditing firm, and secretary general of the organization.

XI. THE ASSOCIATION RULES

a. Associations must keep records of all correspondence.
b. Files must contain name, address, age, date of membership, occupation, and the amount of dues made for all members.
c. Minutes of all the meetings must be kept at headquarters.
d. Must keep a record of all financial statements, budgets, and money raised, its sources and how it is spent.
e. The association must have registered legal council.
f. The finances of the association must be kept at banks within the KSA, and withdrawals must have signatures from two members in the association. These two must be recognized as those enabled to withdraw funds in the association bylaws and organizational chart.
g. The association must put its name, identification number and jurisdiction in all files, correspondences and printouts.

XII. SUBSIDIES AND DONATIONS

a. The MLSA provides the association with statutory subsidies.
b. Charities are able to raise funds and accept donations, and accept will bequests, in the condition that such bequests are in accordance with the laws of the kingdom.

XIII. The MLSA can set up management contracts with charities to enable them to use its offices and pay the MLSA to run its offices.

XIV. NULLIFICATION OF ASSOCIATIONS

Members of association can decide to nullify it according to rules contain on its organizational chart.

XV. THE MLSA CAN DECIDE TO NULLIFY ASSOCIATIONS UNDER THE FOLLOWING CONDITIONS:

a. If the number of members of the association drops below 20.
b. If the association is not respecting its goals or commits fraud or crimes.
c. If the association is not able to meet its financial commitments.
d. If the association transgresses its organizational chart.
e. Fails to respect commonly accepted cultural behavior.
f. The MLSA can appoint a new board of directors to associations.

XVI. ASSOCIATION FINANCES

a. Association members responsible for managing association finances cannot use those funds for personal use.

b. The MLSA provides the rules for association liquidation and will decide who will receive liquidated assets in case it is not clearly stated in the charity's charter.

XVII. MLSA JURISDICTION

a. The MLSA is the official organization in charge of supervising the activities of charities and the implementation of its plans. They have the right to review all files and registers. If an MLSA officer presents himself and requests information about the association, the association must provide this officer with such information.

b. The MLSA has the authority to block any decision emanating from the association that is in opposition to the organizational chart.

XVIII. GENERAL CABINET FOR THE CIVILIAN SERVICE

The MLSA and the General Cabinet for the Civilian Service are in charge of providing certificates and authorization to any citizen who uses any cultural, educational or other type of service provided by charities.

XIX. CREATION OF THE INSTITUTION AND ITS GOALS

It is possible to create a charitable institution for a non-pecuniary goal with the condition that this institution profits only its members or pre-defined groups.

XX. The MLSA has a special file listing all charitable institutions.

XXI. The charitable institution acquires its legal status once registered in this file.

XXII. The same rules organizing charities are applicable to a charitable organization.

XXIII. Charitable institutions cannot receive subsidies from the MLSA nor can they accept small donations (tabarra), but they can still accept large donations (hibet) and receive bequests.

XXIV. After the liquidation of any charitable institution, its money goes to a charitable association according to the directives of the MLSA unless the institutions organizational chart states that proceeds shall go to a specific charitable activity.

XXV. These regulations apply to charitable associations and charitable institutions irregardless of whether they registered or were established prior to the publication of these rules. These regulations do not apply to special charitable institutions created by Royal decree.

XXVI. These regulations emanate from the MLSA and should be announced in the official bulletin.

XXVII. These regulations supercede any conflicting regulations.

XXVIII. These regulations come into effect 60 days after announcement in the official bulletin.

McDermott
Will & Emery

June 30, 2004

BY HAND DELIVERY

The Honorable Susan M. Collins
Chair
Senate Committee on Governmental Affairs
SD-340 Dirksen Senate Office Building
Washington, DC 20510-6250

The Honorable Joseph Lieberman
Ranking Minority Member
Senate Committee on Governmental Affairs
SD-340 Dirksen Senate Office Building
Washington, DC 20510-6250

Re: **June 15, 2004 Committee Hearing on Terrorism Financing**

Dear Senator:

I am writing as counsel to Saudi businessman and benefactor Mr. Yasin Abdullah al Kadi to correct serious and damaging misstatements concerning my client in the Independent Task Force on Terrorist Financing report entitled *"An Update on the Global Campaign Against Terrorist Financing"* released on Tuesday, June 15, ("the Report") during your committee's hearing on current efforts to combat terrorism financing. Most of these misstatements were repeated by Mr. Lee Wolosky, Co-Director of the Task Force, both during his testimony and in responding to questions raised by various Committee members.

As you know, the Report consists of an analysis of ongoing U.S. and Saudi efforts to address terrorist financing and offers recommendations to improve these efforts. One of the Report's main criticisms is that the Saudi government has not taken any *"public punitive actions against any individual for financing terror."*

In making this analysis the Report, as well as Mr. Wolosky's written statement submitted for the record, contains the following statements concerning Mr. Kadi which have caused deep concern to both my client and his entire legal team both in the U.S. and abroad:

> Not only have there been no publicly announced arrests in Saudi Arabia related to terrorist financing, but key financiers remain free or go unpunished. For example, Yasin

U.S. practice conducted through McDermott Will & Emery LLP.
600 Thirteenth Street, N.W. Washington, D.C. 20005-3096 Telephone: 202.756.8000 Facsimile: 202.756.8087 www.mwe.com

> al-Qadi, a Specially Designated Global Terrorist, appears to live freely in Saudi Arabia. *According to the Treasury Department, "He heads the Saudi-based Muwafaq Foundation. Muwafaq is an al-Qaeda front that receives funding from wealthy Saudi businessmen. Blessed Relief is the English translation. Saudi businessmen have been transferring millions of dollars to bin Laden through Blessed Relief.*

See Report at 19, Wolosky Statement at 5 (emphasis added).

This Treasury Department Statement is not publicly available. The Task Force did not properly conduct its due diligence and is instead only once more repeating unsupported statements and allegations made in newspaper articles. For example, it appears that this supposed Treasury Department statement was derived from an October 29, 1999, article entitled "Saudi money aiding bin Laden: Businessmen are financing front groups" by the former and now discredited USA Today Reporter Jack Kelley. As you are likely aware, Mr. Kelley was recently forced to resign after being exposed for fabricating articles, including the October 29, 1999, article referenced above. That article has since been withdrawn by USA Today and is no longer publicly made available.

> A story on Oct. 29, 1999, titled "Saudi money aiding bin Laden," contained several errors. ... The story was written by Jack Kelley, a reporter who was found recently to have fabricated several high-profile stories. In this case, the story's assertions had been widely reported and subsequently retracted by others.

USA Today, p. A2 (Apr. 13, 2004).

The Task Force should have been more careful in verifying its sources, especially when calling for the criminal prosecution of Mr. Kadi. The only proceedings that are currently ongoing in the United States involving Mr. Kadi are civil and administrative proceedings related to OFAC's freezing of his assets. It is irresponsible, and there is no basis for the Task Force to call for a criminal prosecution of Mr. Kadi in Saudi Arabia when criminal charges have not been brought against him in the United States. It is reasonable to presume that criminal charges have not been brought because there is not sufficient evidence to bring such charges or obtain a conviction.

The Committee should insist that the Task Force immediately verify their sources and consult with Mr. Kadi, who they have wrongfully accused but never contacted. Mr. Kadi has always sought a fair and transparent process in which to contest his designation by OFAC. Mr. Kadi reiterates his willingness to meet with Congressional investigators or members of the Task Force.

Mr. Kadi categorically denies any association with terrorism and has, from the beginning, simply sought to clear his name and resume his normal business and philanthropic activities. Mr. Kadi is challenging the freezing measures against him in various countries throughout the world including the U.S., the UK, the European Union, and Switzerland; but these efforts are only further complicated by the careless republication of baseless allegations all over the world.

Mr. Kadi's legal team is challenging the failure to provide any adequate right of redress in a landmark case Mr. Kadi has brought before the European Court of Justice ("ECJ") against the Council and Commission, the institutions of the European Union.

As Mr. Kadi has stated on many occasions that he abhors terrorism and condemns it in all its forms. He is well known within Saudi Arabia as well as in other parts of the world where he has carried on business and is considered to be a respected financier, businessman, and benefactor. Mr. Kadi has never provided support for terrorism, financial or otherwise, and is personally strongly opposed to terrorist activity in all forms. He considers those that support or participate in terrorism to be offensive to the Muslim faith deserving of the most severe condemnation. He believes that those who commit terrorist acts have no place in the Muslim faith.

It is hard to imagine a more serious and damaging charge than complicity with a terrorist organization. As you must appreciate, the continued repetition of already discredited information and the misstatements described above and the insertion in the Congressional record of factual claims that are clearly untrue can only aggravate the harm already suffered by Mr. Kadi, his reputation, his family, and his businesses. This is because the repetition of such allegations in the Congressional Record itself may be used by writers, commentators, and the like to give further credence to false discredited allegations which have no substance in fact no matter how often they are repeated.

Considering the seriousness of this matter, I respectfully request that this letter be made part of the Committee's official record for the June 15, 2004, hearing, and that it be posted on the Committee's website. In addition, the Committee should seek clarification of the Task Force position after it has had an opportunity to further review the issues related to Mr. Kadi.

Sincerely,

Stanton D. Anderson

WDC99 942828-1.064622.0011

William F. Wechsler
Lee S. Wolosky, Esq.

August 3, 2004

Stanton D. Anderson, Esq.
McDermott Will & Emery
600 Thirteenth Street, N.W.
Washington, D.C. 20005

Dear Mr. Anderson:

We write in response to your letters dated June 30, 2004 and July 1, 2004. Those letters were addressed to Senators Susan M. Collins and Joseph Lieberman and to us, respectively.

Your letters expressed certain concerns regarding the recent report of the Independent Task Force on Terrorist Financing sponsored by the Council on Foreign Relations, titled *Update on the Global Campaign Against Terrorist Financing* (the "Report"). Your letters also expressed concerns regarding related Congressional testimony before the Senate Governmental Affairs Committee on June 15, 2004.

We write in our individual capacities, as the principal authors of the Report. We are not writing on behalf of the Council on Foreign Relations, the Task Force, its individual members or its Chairman.

As far as your client Mr. Yasin al Qadi is concerned, the Report quotes from a widely distributed Treasury Department Fact Sheet released on October 12, 2001, when President George W. Bush designated Mr. al Qadi a "Specially Designated Global Terrorist" pursuant to authorities granted to the President under the International Emergency Economics Power Act ("*IEEPA*"). We assume that you have a copy of this Fact Sheet but would be happy to provide a copy to you if you so wish.

As you may know, under IEEPA the President may act against persons he determines to constitute an "unusual and extraordinary threat" to the national security of the United States. As a result of Mr. Qadi's designation by the U.S. government as a "global terrorist," his assets subject to U.S. jurisdiction were frozen and U.S. persons were prohibited from transacting business with him.

Following Mr. Qadi's designation by the U.S. government as a "global terrorist," the United Nations took similar action against him. Notably, the Kingdom of Saudi Arabia supported this multilateral action, according to the United States. In a January 22, 2004 announcement, the Treasury Department noted that, among Saudi Arabia's "important and welcome steps to fight terrorist financing" was the fact that it had "supported the

addition of the Jeddah-based terrorist financier, Yasin Al-Qadi, to the UN's consolidated list in October 2001."

The Report also relied on the following recent statements by current and former senior U.S. government officials concerning Mr. Qadi:

- "... key terrorist financiers and facilitators have had their assets frozen and/or have been arrested or otherwise addressed through the international community's concerted law enforcement efforts. Included in this category are Saudi millionaires Yasin al-Qadi..."

  Testimony of Daniel L. Glaser, Director of the Executive Office for Terrorist Financing & Financial Crimes, before the House Government Reform Subcommittee on Criminal Justice, Drug Policy and Human Resources, May 11, 2004.

- "Key terrorist financiers and facilitators, such as Saudi-millionaires Yasin al-Qadi...have had their assets frozen and/or have been arrested or otherwise addressed through the international community's concerted law enforcement efforts."

  Testimony of Juan C. Zarate, Deputy Assistant Secretary Executive Office for Terrorist Financing & Financial Crimes, before the Senate Caucus on International Narcotics Control, March 4, 2004.

- "Yasin al Qadi is allegedly the financier behind several U.S. organizations which have been tied to terrorist support. Qadi has been identified in court papers as the banker behind a convoluted real estate transaction in Illinois where proceeds where siphoned off to Hamas operatives. Qadi has also been reported to be a lead investor in BMI, a New Jersey based Islamic investment bank catering to ranking members of the Muslim Brotherhood, including Hamas and al Qida backers. In October 2001, the Treasury department listed Yasin al Qadi as a designated terrorist for his financial support of al Qida. Qadi was the head of Muwafaq, a Saudi "relief organization" that reportedly transferred at least $3 million, on behalf of Khalid bin Mahfouz, to Usama bin Laden and assisted al Qida fighters in Bosnia."

  Testimony of Richard A. Clarke, National Coordinator for Counterrorism under Presidents George W. Bush and William Jefferson Clinton, before the Senate Banking Committee, October 22, 2003.

As should be clear, Mr. Qadi should raise his objections directly with the U. S. government and the United Nations. If and when the U.S. government and the United Nations change their judgments of Mr. Qadi, we would be happy to consider making any necessary revisions to the Report.

We note that you have asked that your letters to Senators Collins and Lieberman be placed into the Senate record and posted on the website of the Senate Governmental Affairs Committee. We are asking that this same treatment be afforded to this response, along with a November 29, 2001 letter from the Treasury Department to the Swiss authorities that further elaborates the basis upon which the U. S. government designated Mr. Qadi a "global terrorist."

Sincerely,

William F. Wechsler

Lee S. Wolosky, Esq.

cc: The Honorable Susan M. Collins
The Honorable Joseph Lieberman
Maurice Greenberg
Richard Haass
Harvey W. Freishtat, Esq.
Members of the Task Force

DEPARTMENT OF THE TREASURY
WASHINGTON

GENERAL COUNSEL

November 29, 2001

M. Claude Nicati
Substitut du Procureur General
Taubenstrasse 16
3003 Berne
SWITZERLAND

Re: Yassin A. Kadi

Dear Mr. Nicati:

This letter is provided to you pursuant to your request under the mutual legal assistance treaty between the United States and Switzerland in connection with the action taken by the Government of Switzerland to block assets of Yassin A. Kadi (aka Qadi or Qadhi). Although some of the information concerning Mr. Kadi comes from sensitive sources that we cannot disclose, we have agreed to provide you with an unclassified summary of certain information concerning Mr. Kadi. We believe that this information is generally reliable and, taken as a whole, supports the decision to block Mr. Kadi's assets. This summary may be disclosed publicly in legal proceedings.

Based upon information available to the United States Government, we have a reasonable basis to believe that Mr. Kadi has a long history of financing and facilitating the activities of terrorists and terrorist-related organizations, often acting through seemingly legitimate charitable enterprises and businesses.

In 1991, Mr. Kadi wired $820,000 to a business in the United States. This money was laundered through a complex land transaction in Illinois, apparently to hide any connection to Mr. Kadi and the eventual transfer of the funds to the Quranic Literacy Institute (QLI). Some of the proceeds of this transaction were used by QLI to finance the activities of Mohammed Salah (alias Abu Ahmed),[1] an admitted head of the military wing of the terrorist organization HAMAS.[2] Subsequently, Mr. Kadi wired $27,000 *directly* to Mr. Salah's account in March

---

[1] Mr. Salah is a "Specially Designated Terrorist" (SDT) under United States Executive Order No. 12947, 60 Fed. Reg. 5079 (1995) (E.O. 12947). See Notice of Blocking, 60 Fed. Reg. 41152 (1995).

[2] HAMAS has been designated a "Foreign Terrorist Organization" pursuant to the Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. 104-132, 110 Stat. 1214 (1996) and an SDT under E.O. 12947, see 31 C.F.R. Ch V, App. A, and a "Specially Designated Global Terrorist" (SDGT) under United States Executive Order No. 13224, 66 Fed. Reg. 49079 (2001) (E.O. 13224).

1992. This wire, from Faisal Finance account number IFA 10004, came directly from an account that is the subject of the Swiss sequestration order covering Mr. Kadi's accounts. There were additional wires from Faisal Finance to Mr. Salah's account, but our information on those transfers is still incomplete. Similarly, we are still investigating other Faisal Finance transfers, one for $200,000 and another for $665,000, all or a substantial portion of which were sent to Mr. Salah through an account controlled by another HAMAS operative, Abu Marzook.[3]

At the direction of Abu Marzook, Mr. Salah distributed tens of thousands of dollars, and perhaps more, to HAMAS cells in and around Israel. Mr. Salah was arrested in Israel in 1993 carrying nearly $100,000 in cash and extensive notes of his meetings with HAMAS operatives during the days preceding his arrest. Analysis of the monetary transfers involved in the Illinois land transaction, and of wires into Mr. Salah's accounts prior to leaving for Israel, show a close connection between the funds involved in the transactions and those distributed by Mr. Salah to terrorist cells.[4]

In recent press interviews, Mr. Kadi has denied any wrongdoing in connection with these money transfers. He says that the loan on the Illinois property was intended to help the QLI "open a peaceful dialogue between nations," but he has neither explained the convoluted nature of the transaction nor made any claim for repayment of the "loan." He claims not to recall ever having met Mr. Salah, although Mr. Salah's lawyer states that Mr. Salah did meet with Mr. Kadi, that Mr. Kadi befriended him, and that he gave the $27,000 to Mr. Salah to open a bank account in Chicago.

Mr. Kadi has acknowledged in a number of press accounts that he is the founder of the Muwafaq, or "Blessed Relief," Foundation. He is identified in legal records as "Chairman" of the foundation. The leader of the terrorist organization Al-Gama'at Al-Islamiya,[5] Talad Fuad Kassem, has said that the Muwafaq Foundation provided logistical and financial support for a mujahadin battalion in Bosnia. The foundation also operated in Sudan, Somalia and Pakistan, among other places.

A number of individuals employed by or otherwise associated with the Muwafaq Foundation have connections to various terrorist organizations. Muhammad Ali Harrath, main activist of the Tunisian Islamic Front (TIF) in the United Kingdom, was associated with Muwafaq personnel in Bosnia and other TIF members worked at the Muwafaq Foundation. Syrian citizen Mahmoud Mehdi, once a director of the Muwafaq Foundation in Pakistan, was a member of Al-Qa'ida and the Al-Furan terrorist group[6] responsible for the kidnapping of

---

[3] Mr. Marzook has been designated a SDT under E.O. 12947. See 31 C.F.R. Ch. V, App. A.

[4] A detailed account of Mr. Salah's activities, which included the recruitment and funding of HAMAS terrorists, can be found in the affidavit of FBI Special Agent Robert Wright (previously provided to you) and in *In re Extradition of Marzook*, 924 F. Supp. 565, 587-92 (S.D.N.Y. 1996).

[5] Al-Gama'at Al-Islamiya has been designated a "Foreign Terrorist Organization" pursuant to the Anti-Terrorism and Effective Death Penalty Act of 1996. See 31 C.F.R. Ch. V, App. A.

[6] Al-Furan is a "Specially Designated Global Terrorist Entity" under E.O. 13224.

Westerners in Kashmir. He was also close to Ramzi Yusif who has been convicted in the United States for his role in the first World Trade Center attack. Following the arrest of Ramzi Yusif in 1995, the Pakistani police reportedly raided Muwafaq's offices and held its local director in custody for several months. The Muwafaq Foundation also provided support to HAMAS and the Abu Sayyaf Organization[7] in the Philippines.

The Muwafaq Foundation also employed or served as cover for Islamic extremists connected with the military activities of Makhtab Al-Khidamat (MK),[8] which has been partially financed by the Muwafaq Foundation. The Muwafaq Foundation supplied identity cards and employment as cover for some Arabs to allow them to obtain visas to remain in Pakistan. The founder of MK was Abdallah Azzam, who was Usama bin Laden's mentor. Following the dissolution of MK in early June 2001 and its absorption into Al-Qa'ida, a number of NGOs formerly associated with MK, including Muwafaq, also merged with Al-Qa'ida.

Mr. Kadi has asserted in various press interviews that the Muwafaq Foundation ceased operations at a range of different times in 1995, 1996 or 1997. However, the United Nations reported that Muwafaq was active in Sudan as late as 1997. Moreover, far from ceasing operations, the U.N. report stated that the "Muwafaq Foundation plans to *continue to expand* its humanitarian activities in the coming year . . . ." U.N. Department of Humanitarian Affairs, *Consolidated Inter-Agency Appeal for Sudan January-December 1997* (Feb. 18, 1997)(emphasis added).

From 1993, the head of the European offices of the Muwafaq Foundation was Ayadi Chafiq Bin Muhammad, who has been identified as Mr. Kadi's closest associate.[9] Ayadi Chafiq fought in Afghanistan in the 1980s and is known to be associated with the Tunisian Islamic Front (TIF) in Algeria and Nabil Ben Mohammad Salah Makloul, its leader. Mr. Chafiq was expelled from Tunisia because of his membership in the TIF. As of February 1999, Mr. Chafiq was running Mr. Kadi's European network and serving as the president of Depositna Banka in Sarajevo, Bosnia, which was owned by Mr. Kadi. Mr. Chafiq may have participated in planning an attack on a U.S. facility in Saudi Arabia. Mr. Chafiq left his residence in London in a hurry after the September 11 attacks, and had reportedly been in the United States in the months preceding the attack.

The pattern of activity displayed by Mr. Kadi, and his foundation and businesses, is typical of the financial support network of Al Qa'ida and other terrorist organizations. Working in troubled areas such as Bosnia, Somalia, Sudan, and various refugee camps, the putative "relief" organizations provide cover for individuals engaged in recruiting, organizing, and

---

[7] The Abu Sayyaf Organization is a "Specially Designated Global Terrorist Entity" under E.O. 13224.
[8] MK is a "Specially Designated Global Terrorist Entity" under E.O. 13224.
[9] Ayadi Chafiq is a "Specially Designated Global Terrorist Individual" under E.O. 13224. See Amendment of Final Rule, 66 Fed. Reg. 54404 (2001). He also is listed as one of the signatories on Swiss accounts at Faisal Financial with Kadi.

training terrorist cells. Their provision of humanitarian aid and educational services is done in concert with the terrorists to win the hearts and minds of the local people to whatever causes the terrorists espouse. When a region becomes more settled, such as Bosnia or Albania today, seemingly legitimate businesses replace charitable foundations as cover for continuing terrorist organizational activity. Mr. Kadi's actions and those of his Muwafaq Foundation and businesses fit this pattern and give rise to a reasonable basis to believe that they have facilitated terrorist activities.

As noted previously, this is a summary of information concerning Mr. Kadi that we can release at this time. If we are able to release additional information in the future we will let you know.

Sincerely,

David D. Aufhauser
General Counsel